The USA PATRIOT Act of 2001: A Case Study Analysis

by

Irene Denney

Submitted in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Criminal Justice

YOUNGSTOWN STATE UNIVERSITY

December, 2023

The USA PATRIOT Act of 2001: A Case Study Analysis

Irene Denney

I hereby release this thesis to the public. I understand that this thesis will be made available from the OhioLINK ETD Center and the Maag Library Circulation Desk for public access. I also authorize the University or other individuals to make copies of this thesis as needed for scholarly research.

Signature:

_____

Irene Denney, Student Date

Approvals:

_____

Dr. Christopher Bellas, Thesis Advisor

Date

_____

Dr. Monica Merrill, Committee Member Date

_____

Captain Jason Simon, Committee Member Date

_____

Dr. Salvatore A. Sanders, Dean, College of Graduate Studies Date

DEDICATION

To my committee—Dr. Christopher Bellas, Dr. Monica Merrill, and Captain Jason Simon.

To my amazing family who provided me with invaluable support throughout this adventure.

To all others who believed in me.

Abstract

The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* Act*,* more widely known as the USA PATRIOT Act of 2001, is a groundbreaking piece of legislation that was swiftly enacted in response to the terrorist attacks against the World Trade Center and the Pentagon on September 11, 2001. The USA PATRIOT Act of 2001 consists of ten different sections of text thoroughly detailing redesigned governmental functions, all of which generally aim to prevent, mitigate, and eliminate the threat that terrorism poses against the United States and its citizens. The second section, known as Title II: Enhanced Surveillance Procedures, expanded federal law enforcement's authority to conduct more thorough surveillance of terrorist activity. This thesis is guided by the following research question: How has the USA PATRIOT Act of 2001 impacted the way that federal law enforcement conducts the surveillance of terrorist activity in the United States? For this thesis, the methodology and design consists of an explanatory, single-case study which investigates and analyzes Title II of the USA PATRIOT Act of 2001 within the context of surveillance counterterrorism measures implemented by federal law enforcement in the United States. This thesis builds upon preexisting counterterrorism literature and is beneficial to future studies which attempt to thwart the perpetual fight against terrorism and strengthen national defense against foreign and domestic enemies.

Table of Contents

Chapter 1 – Introduction

"This is a day when all Americans from every walk of life unite in our resolve for justice and peace. America has stood down enemies before, and we will do so this time. None of us will ever forget this day. Yet, we go forward to defend freedom and all that is good and just in our world."

--President George W. Bush's Address to the Nation on September 11, 2001

9/11

For many Americans, the sunrise in the early morning on September 11, 2001, simply and innocently dawned another day of work. Professionals with well-established careers at the World Trade Center in New York City and at the Pentagon in Arlington County, Virginia, were only getting their day started, as one of the most horrific events in U.S. history was about to unfold before their own eyes. The World Trade Center (WTC) was a group of seven buildings located in Lower Manhattan in NYC. These important structures were housed in the Financial District and served as an unwavering symbol of the sheer power of the American economy. The Twin Towers were part of the WTC and consisted of the North (1 WTC) and South Tower (2 WTC). These buildings, along with 7 WTC and the Pentagon, would be the target of the deadliest terrorist attack in United States history.

At approximately 8:46 A.M., al Qaeda terrorists crashed the hijacked American Airlines Flight 175 into floors 93-99 of the North Tower (9/11 Commission Report, 2004). Building evacuation alarms alerted everyone inside, however, the activated system was not working in many areas of the building due to damage from the crash. Instantly, the emergency dispatch lines were overwhelmed with an insurmountable number of calls from people both in and outside of the towers. Initially, people who called 911 were told to remain in their location and await further

instructions from authorities. Evidently, due to ineffective and improper evacuation advice and general knowledge of the situation at hand, tenants in the North Tower were merely instructed to stay low and wait for first responders to find them and aid in evacuation measures. Nonetheless, FDNY (New York Fire Department) chief personnel ordered an immediate and total evacuation of the North Tower and, by 8:57 A.M., an evacuation of the occupants in the South Tower, since the degree of damage and destruction to 1 WTC was such a devastating impact. The issue at this point was that these major executive decisions were never sent to 911 and FDNY dispatchers.

Amid the chaos and smoke plumes covering the streets and skies, there were numerous instances of faltering, inconsistent instructions and substantial deviation from protocol on behalf of first responders and dispatchers. This led to widespread confusion and only further complicated the process of aid and evacuation. In addition, those trapped in the North Tower encountered obstacles such as thick black smoke, the stifling scent of jet fuel filling the air, and rooms and hallways that were blocked by debris from the impact of the plane. A lot of the stairways that were able to be accessed were soon crowded with people rushing to safety. Groups such as the elderly and the disabled were faced with even more panic as the stairs got packed and elevators no longer worked.

Meanwhile, in the South Tower, there was an announcement system that notified its occupants that the incident was isolated in the North Tower, that they were safe, and how they should return to their designated workplace. Ultimately, no one was expecting that another hijacked plane would soon strike 2 WTC. At 9:02 A.M., the overhead alert system declared that if individuals deemed the current situation bad enough, an evacuation could proceed. Only one minute later, at 9:03, a second plane (United Airlines Flight 175) being piloted by terrorists would crash into floors 77-85 of the South Tower.

Severe and substantial structural damage to the North Tower prevented a helpful escape tool from being utilized; there was a “lock release” order initiated at 9:30 by a group known as the Security Command Center, which was conveniently located in 1 WTC. Unfortunately, the impact of the plane interrupted and subsequently destroyed this system which would have unlocked all doors and vital access points, facilitating a smoother evacuation. This was only one of the many complications which arose. In addition, the 911 emergency dispatch lines received an overwhelming influx of phone calls from witnesses. These services were not equipped with the ability to handle a situation of this magnitude. Everyone was in a state of either shock, panic, disbelief, fear, or a pure combination of all. This attack on innocent American lives was unprecedented and unimaginable. Many individuals, stuck in both towers, saw no other possible way out of their demise and resorted to jumping to their death.

On the ground, units of the FDNY were scattered and scrambling in a fruitless attempt to execute a search-and-rescue operation inside both the North and South Tower. Communications between commanding posts and emergency personnel were greatly impaired by the utter madness and confusion ensuing. These events were like no other, and not a single person could have predicted the level of destruction, death, and disorder that would follow this disaster. So many groups of emergency responders came to the scene to aid, but this crowding of professionals made it practically impossible for higher-ups to keep track of each unit and properly direct them.

The New York Police Department (NYPD) dispatched around 2,000 officers on foot to aid with the evacuation of the towers while they were still standing. Over a thousand police from the Port Authority of New York and New Jersey Police Department were also at the scene right beside the NYPD, helping to mitigate the chaos and tragedy around them. Horrifically, at 9:59

A.M., the South Tower began to collapse from the exceptional damage it had endured. Mass panic, horror, and confusion multiplied in an instant. Within a matter of seconds, the entire structure was reduced to piles of debris and clouds of dense smoke, ash, and pulverized building materials, which claimed the lives of many innocent Americans in its way. In an instant, the modicum of structure and cooperation between command posts was gone. The terror and shock of this unfolding situation caused even more disarray for those responders that were trying to dissent advice to panicked callers. Proper emergency evacuation protocol was abandoned in the fear-fueled chaos. At this time, the FDNY was encouraging the firefighters to flee from the North Tower due to an imminent risk of total building collapse. At 10:28 A.M., 1 WTC could no longer withstand the kind of impact it took and crumbled to the ground. Most of the civilians and first responders in the tower were instantly killed when the building toppled.

While these tragic events were unfolding in New York City, another sinister attack would be felt at the Pentagon in Virginia. At 9:37 A.M., the Pentagon was struck by a terrorist-hijacked plane. This American Airlines Flight 77 was the third commercial plane that day which al Qaeda members captured and used in their efforts to cause as much death and devastation as possible. All passengers on the flight passed away on impact as well as 125 individuals within the Pentagon. Contrary to the response to the attack on the Twin Towers, the overall reception and response to the attack on the Pentagon was much swifter, clearer and more organized — this was due to the coordinated efforts of all command posts, first responders, and involved government personnel (9/11 Commission, 2004). The communication between the officials regarding the situation at the Pentagon was substantially more established and streamlined. Within minutes, lines of communication between commands were utilized to make an alert that a complete evacuation of the building was not only necessary, but imminent.

This was not the last of the terror. While New York and Virginia were under attack, four hijackers captured United Airlines Flight 93 with the intention of crashing the plane into either the Capitol building or the White House. One of the four men, named Ziad Jarrah, overtook controls in the cockpit and began piloting the aircraft. This situation was unique from the other three flights that had been hijacked that day. By the time that Flight 93 was overtaken by terrorists, passengers had caught word of the attacks against the World Trade Center through phone calls with their friends, family, and coworkers. A plot was devised amongst those still alive onboard to overthrow the terrorists by launching a coordinated effort to charge at them in the cockpit and, perhaps, be able to bring the plane to safety. Those brave men and women that attacked the hijackers with everything in their power prevented the terrorists from crashing the plane into another building. The barrage caused the hijackers piloting the aircraft to lose control, ultimately leading to its fateful impact on an empty field in Shanksville, Pennsylvania at 10:03 A.M., where all passengers and crew would perish instantly. The unforgettable efforts of those passengers helped thwart the sinister agenda that was looming.

In total, 2,973 lives were lost on that fateful day (9/11 Commission, 2004). Four commercial airplanes would be hijacked by a total of nineteen terrorists with the intention of causing mass death, destruction, and degradation to the United States, its citizens, and the integrity of its democracy. September 11, 2001, became a turning point in American history. Any semblance of personal comfort was disintegrated. U.S. citizens developed a newfound fear of terrorism that had never been so intense. Millions of Americans witnessed the planes making impact with the North and South Tower of the World Trade Center on live television, even in schools and workplaces. The horror was being broadcast on every operating news station across the country. 9/11 would serve as the largest, most deadly terrorist attack to ever happen on U.S.

soil (9/11 Commission, 2004). Amidst the devastating aftermath of this day, the American people were left to wonder, "What happens next?" The 9/11 terrorist attack impacted U.S. defense by exposing weak areas in the system and subsequently affecting the way that Americans perceive health and safety. The federal government knew that some type of action was to be taken to prevent this type of situation from ever happening again. There became an immediate need to help the victims of this tragedy, return air travel back to normal while increasing security measures, and restore the integrity of the United States as a whole. President George W. Bush gave a nationally televised speech on the night of 9/11, stating his intent of prioritizing aid for affected persons as well as mitigating and preventing future attacks (9/11 Commission, 2004; The White House, 2001). An additional need for overarching legislation in support of countering future terrorist acts while mitigating the effects of 9/11 became apparent. Within days, a draft of a piece of legislation that would eventually be known as the USA PATRIOT Act of 2001 was born.

In summary, the 9/11 terror attacks consisted of nineteen al Qaeda terrorists hijacking four commercial airplanes with a result of nearly 3,000 American lives being lost. The integrity of democracy was tarnished by their actions of targeting critical structures in the United States that symbolized the nation's power and prowess. At 8:46 A.M., the North Tower of the World Trade Center (1 WTC) in New York City was hit by American Airlines Flight 11, piloted by terrorist Mohamed Atta; everyone on the flight perished including many who were occupying the North Tower at the time. At 9:03 A.M., the South Tower of the World Trade Center (2 WTC) was struck by United Airlines Flight 175, piloted by terrorist Marwan al Shehhi; all passengers and crew died instantly, along with those inside the building. Around 9:37 A.M., American Airlines Flight 77, piloted by terrorist Hani Hanjour, collided into the side of the Pentagon in Arlington,

Virginia, ending the lives of all passengers and crew on board as well as 125 individuals inside the Pentagon. At 9:59 A.M., 2 WTC collapsed, killing all civilians and first responders inside the building. When 10:03 A.M. came, United Airlines Flight 93, piloted by terrorist Ziad Jarrah, crashed into an open, empty field in Shanksville, Pennsylvania; forty people perished, including the hijackers. 1 WTC collapsed at 10:28 A.M., killing all occupants.

The effect of these terrorist attacks was instantaneous as waves of fear, anger, sadness, and uncertainty swept through every facet of American lives. The United States and its people were wholeheartedly unprepared for a catastrophe of such magnitude. In the eyes of the government, as well as the people, there became an imminent need to establish official counterterrorism strategies and legislative guidelines that would be able to sufficiently tackle the threat that terrorism poses, as well as prevent and mitigate future terrorist attacks. It was clear that an overarching piece of legislation with this intent in mind would be the next step in rebuilding and restoring the nation from the heinous events of 9/11. The terrorist attacks on September 11, 2001, were significant and unique in the sense that they were so tragic that they led to the creation of the USA PATRIOT Act of 2001 only one month later (9/11 Commission, 2004). Congress was in a rush to push legislation out in response to the attacks, so there was little debate regarding the passage of the Act (Deflem & McDonough, 2015). The USA PATRIOT Act of 2001was enacted by Congress with bipartisan support; it passed through the Senate with a vote of 98-1 and through the House with a vote of 357-66 (DOJ, 2023). After weeks of struggling to repair the nation after such a critical hit, President George W. Bush signed the USA PATRIOT Act of 2001 (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct* Terrorism) of 2001 into law on October 26, 2001. The purpose of the USA PATRIOT Act of 2001, as emphasized in the introduction to this legislation,

is “To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes” (Pub. L. 107-56 2001). The enactment of the USA PATRIOT Act of 2001 was preceded by the passing of similar legislation such as the Communications Act of 1934, the Omnibus Crime Control and Safe Streets Act (Wiretap Act) Act of 1968, and the Foreign Intelligence Surveillance Act (FISA) of 1978 (Bellas, 2012). The purpose of the Communications Act is, “To provide for the regulation of interstate and foreign communications by wire or radio…” (Pub. L. 117-338, (1934)); this Act regulated the communications industry. The Wiretap Act was enacted to, “…assist State and local governments in reducing the incidence of crime, to increase the effectiveness, fairness, and coordination of law enforcement and criminal justice systems at all levels of government….” (Pub. L. No. 90-351, (1968)); this Act established specific guidelines and provisions that involve provisions for law enforcement assistance and wiretapping and electronic surveillance. Finally, the Foreign Intelligence Surveillance Act established procedures for the authorization to use electronic surveillance, pen register and trap and trace devices, searches, and to gather personal records for the purpose of obtaining foreign intelligence information.[1]

The deliberate emphasis on the enhancement of tools utilized by law enforcement in their investigation of terrorist activity serves as the crux of this thesis, since the goal of the research question is to determine how the enhanced tools under Title II have impacted the monitoring and surveillance of terrorist activity by federal law enforcement. Despite the clear efforts to return to normalcy following the most heinous terrorist attack on U.S. soil, Americans were still left to wonder if, perhaps, the government failed to recognize any warning signs of Osama bin Laden and/or al Qaeda’s intention to commit such an attack against the United States. In the years

[1] *Pub. L. 95-511*

before 2001, the degree of intelligence sharing amongst governmental entities and federal law enforcement agencies was not nearly as sophisticated as it was following the enactment of the USA PATRIOT Act of 2001. In April of 2004, the United States government's intelligence community declassified and released a report to the public titled "Bin Laden Determined To Strike in US" which emphasized the impending threat of Osama bin Laden and his terrorist organization known as al Qaeda. This report was a memo in the Presidential Daily Brief, dated August 6th, 2001, that was created by the Central Intelligence Agency (CIA), and was directed *solely* at President George W. Bush. This memo harrowingly described bin Laden's tenacity regarding his terrorist operations and attacks throughout the years that, despite not always being successful, such setbacks have proven to not be a deterrent for him (Presidential Daily Brief, 2001). The most disturbing element of this memo was the mention of a report only three years prior to the 9/11 attacks where bin Laden supposedly stated his intention of hijacking a U.S. aircraft (Presidential Daily Brief, 2001). This Presidential Daily Brief (2001) is concluded by the intelligence community's deliberate emphasis on the FBI's efforts to conduct nation-wide investigations related to Osama bin Laden and his terrorist capabilities due to "…patterns of suspicious activity in this country consistent with preparations with hijackings…including recent surveillance of federal buildings in New York." This information was obviously disturbing for many people when they realized that the U.S. government was aware, to a certain extent, of bin Laden and/or al Qaeda's intention to commit a terrorist attack on U.S. soil. In fact, the briefing acknowledges that, across New York, terrorist cells headed by bin Laden and his counterparts were involved in the recruitment of Muslim-Americans into al Qaeda (Presidential Daily Brief, 2001). This memo brought to light the failure of the government in recognizing the warning signs of a possible terrorist attack prior to that of 9/11. Perhaps, if the information discussed

throughout this briefing was brought to the attention of more governmental entities than just the President, federal law enforcement agencies might have had an opportunity to prepare for a potential terrorist attack. A significant purpose of the USA PATRIOT Act of 2001 is to facilitate intelligence-sharing amongst federal law enforcement and government agencies by "…enhanc[ing] law enforcement investigatory tools" (Pub. L. 107-56 2001).

A case study analysis of the USA PATRIOT Act of 2001 serves as the basis for this thesis. The nature of this case study involves causal or explanatory research in which the extent and nature of the cause-and-effect relationship between Title II of the USA PATRIOT Act of 2001 and how federal law enforcement conducts surveillance of terrorism and terrorist activity. The September 11th terrorist attacks were evidence that U.S. national defense was not impenetrable. The unprecedented horror that ensued on that day sparked an instantaneous change in American history and essentially reshaped the structure of national defense. The focus of the later chapters is to scrutinize Title II: Enhanced Surveillance Procedures under the USA PATRIOT ACT OF 2001 and, ultimately, assess how this legislation has impacted the way that federal law enforcement officers and investigators conduct surveillance of terrorist activity. Law enforcement agencies, investigators, and officers have become significantly more involved in U.S. counterterrorism strategies since 9/11. This thesis contributes to the continuing efforts of combatting terrorist attacks on U.S. soil by providing extensive insight into perhaps the most significant piece of terrorism legislation enacted after the September 11, 2001, attacks. This topic is worthy of study considering the catastrophic magnitude of the events that transpired that day, which affected not only the United States, but countries around the world. The cataclysmic attack on the World Trade Center and the Pentagon triggered a war on terror, officially labeled the "Global War on Terrorism" (U.S. Department of State Archive, 2009). The following chapter

reviews the literature on topics of the USA PATRIOT Act of 2001, national defense, counterterrorism, surveillance procedures, and 9/11.

Chapter 2 – Literature Review and Theory

Robert K. Yin, an expert in case study methodology, emphasized that the first step in developing a case study is to conduct a literature review.[2] This chapter consists of a literature review on numerous significant articles, research studies, and government publications that are relevant to topics such as international and domestic terrorism, the USA PATRIOT Act of 2001, 9/11, surveillance, counterterrorism, homeland security/ national defense, and radicalism/extremism. The purpose of this Chapter is to review the literature on these topics and prepare the reader for the remainder of the thesis/case study analysis by providing them with critical insight on these concepts.

National Strategy for Counterterrorism. The first publication is directly related to the implementation of surveillance procedures as counterterrorism measures. The source is known as the *National Strategy for Counterterrorism* (NSC) and is a comprehensive strategical outline adopted by the United States government. The NSC builds upon the previously constructed *National Security Strategy* (NSS). The NSC is composed of a three-fold plan that consists of a strong focus on tackling the ever-growing threats surrounding both foreign and domestic acts of terrorism. The overall purpose of the NSC is to provide a way for the United States to mitigate and conquer terrorism and extremism, which can only occur if there are established relationships and connections between the U.S. and public, private, and foreign sectors. There is a list of six

[2] Yin, R.K. (2003). Case Study Research: Design and Methods. Third Edition, p. 156
Yin, R.K. (2014). Case Study Research: Design and Methods, Fifth Edition, p. 3

total “lines of effort” which are the ultimate means for achieving four “desired end-states” which coincide with the goal of eliminating terrorism and violent extremism (ODNI, 2018). One line of effort defined in the NSC states the intention of destroying and interrupting the various entities that terrorists rely on, such as financial, material, and logistical sources (ODNI, 2018). Another line of effort is countering radical/extremist recruitment amongst terrorists and terrorist groups, which is the means of achieving the third end state listed in the introduction where such ideologies do not threaten the American people and the democracy of the United States. The NSC emphasizes their efforts to combat terrorism through surveillance and information sharing. For example, the plan states their goal to “...improve the ability to share timely and sensitive information on threats and the individuals perpetrating them, whether motivated by domestic or foreign terrorist ideologies, across all levels of government. We will continue to ensure that law enforcement agencies across all levels of government have the information that they need to identify and act swiftly against terrorist activity” (ODNI, 2018). The declaration of that intent to increase information-sharing with private sectors and to remove existing obstacles to this action proves there is an emphasis on surveillance, although this specific term is not utilized. Title II: Enhanced Surveillance Procedures under the USA PATRIOT Act of 2001 describes law enforcement’s authorities to intercept wire, oral, and electronic communications relating to terrorism and computer abuse, in addition to the authority to share criminal investigative information (§ 201-203. Pub. L. No. 107-56 2001). Thus, it is logical to assume that the sharing of information in which the *National Strategy for Counterterrorism* describe, coincides with a certain degree of surveillance. Another purpose of the NSC is to educate and prepare American citizens on the topics of terrorism and counterterrorism; it is logical to assume that increased education would facilitate greater public cooperation with government counterterrorism

strategies. It is important to note the NSC's emphasis on domestic terrorism being just as much of a threat as international (foreign) terrorism, if not more. The notions of radicalism and extremism arise throughout the National Strategy for Counterterrorism and are correlated to certain terrorist groups, such as the Islamic State of Iraq and al-Sham (ISIS) and al Qaeda (ODNI, 2018). Conclusively, the NSC emphasizes the growing need to adapt to advancements in technology which have subsequently heightened the threat of terrorism in and against the United States. For instance, the implications of terrorist groups using WMDs (weapons of mass destruction) are both catastrophic and deadly. Thus, the National Strategy for Counterterrorism is an invaluable source to the continued efforts in combatting terrorist activity in the U.S. With the goal of this strategy being to conquer extremism and diminish terrorism, the NSC is concluded by detailing specific priority actions for the federal government to take in their counterterrorism procedures. Such priority actions underlined within the NSC involve the targeting of key terrorists and/or terrorist groups, the enhancement of reach into desired areas overseas, the effective use of law of armed conflict (LOAC) detention as a technique in counterterrorism strategies, and the further integration of information sharing amongst federal, state, and local levels (ODNI, 2018). The three-fold action plan comprised of strategic goals, lines of effort, and end states forms the foundation of the National Strategy for Counterterrorism of the United States and involves creating stronger, impenetrable borders as well as ensuring that critical infrastructure of the U.S. is properly and adequately secured.

Strategic Intelligence Assessment and Data on Domestic Terrorism. This report was published by the Director of National Intelligence through the Department of Justice's Federal Bureau of Investigation and the United States Department of Homeland Security. Domestic terrorism is the sole focus of this publication since the drastic rise in domestic violence

extremists since 9/11 (DNI, 2022). The report defines a domestic violent extremist (DVE) as someone who is "…based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals, wholly or in part, through unlawful acts of force or violence dangerous to human life" (DNI, 2022). Lone offenders and smaller groups of individuals with radical beliefs pose the most significant threat to U.S. national security (DNI, 2022). This has changed the way that federal law enforcement conducts surveillance of terrorist activity because lone-wolf offenders are typically harder to locate than larger, notorious bands of terrorists. There are five distinct categories of domestic terrorism threats that the United States government officially recognizes: racially or ethnically motivated violent extremism, anti-government or anti-authority violent extremism, animal rights/environmental violent extremism, abortion-related violent extremism, and a general division that encompasses all other domestic terrorism threats that do not fall under the previous four categories (DNI, 2022). The category that poses the biggest threat to the homeland is the first one which involves racially/ethnically motivated violent extremists (RMVEs). This source explains how RMVEs justify their radical ideologies for political and/or religious reasons (DNI, 2022). According to a 2021 assessment conducted by the Federal Bureau of Investigation alongside the Department of Homeland Security, RMVEs that advocated for white supremacy and violent, anti-authority/government extremism (i.e., 'militia violent extremists') pose the deadliest threat against the homeland since they are "…most likely to conduct mass-casualty attacks against civilians, and militia violent extremists would typically target law enforcement and government personnel and facilities" (DNI, 2022). It is clear that the United States government is making a concerted effort to focus their counterterrorism strategies on domestic terrorism, since it poses a more significant threat to

national security than international/foreign terrorism did in the years following the 9/11 terrorist attacks (DNI, 2022). This report places an emphasis on the threat posed towards federal law enforcement as it references an incident where an RMVE tried to justify his murdering of a law enforcement officer through his interpretations of religion and religious teachings (DNI, 2022). The report is valuable to counterterrorism research studies in that it explains the various training and resources provided to federal and state, local, tribal, and territorial (SLTT) law enforcement agencies and investigators involved in the U.S. government's assessment and mitigation of domestic terrorism and international terrorism threats. For instance, the Department of Homeland Security's National Threat Evaluation and Reporting Program (NTER) assists federal law enforcement and homeland security officials by providing them with valuable resources and training that helps them better locate, mitigate, and eliminate "…targeted violence and mass casualty incidents implicating homeland security, including those associated with terrorism, as well as facilitating a national capacity for identifying, evaluating, and reporting, and sharing tips and leads related to those threats" (DNI, 2022). The implications of domestic terrorism on federal law enforcement's role in the implementation of U.S. counterterrorism strategies puts a strain on law enforcement and intelligence communities, particularly since the process of monitoring for lone wolf offenders and smaller groups of extremists requires a sophisticated detection system of 'signatures'—characteristics that a suspected DVE would display prior to their committing a terrorist attack (Hamm & Spaaj, 2015).

National Strategy for Countering Domestic Terrorism. In June 2021, the NSCDT (National Strategy for Countering Domestic Terrorism) was published by the National Security Council. This publication is a modern-day example of governmental efforts to ensure protection

of the homeland—this federal report outlines four 'pillars' and underlying strategic goals that align with U.S. counterterrorism goals and strategies:

(I) **Pillar One:** Understand and Share Domestic Terrorism-Related Information

Strategic Goal 1.1: Enhance Domestic Terrorism-Related Research and Analysis.

Strategic Goal 1.2: Improve Information Sharing Across All Levels Within, As Well As Outside, The Federal Government.

Strategic Goal 1.3: Illuminate Transnational Aspects of Domestic Terrorism.

(II) **Pillar Two:** Prevent Domestic Terrorism Recruitment and Mobilization to Violence

Strategic Goal 2.1: Strengthen Domestic Terrorism Prevention Resources and Services.

Strategic Goal 2.2: Address Online Terrorist Recruitment and Mobilization to Violence by Domestic Terrorists.

(III) **Pillar Three:** Disrupt and Deter Domestic Terrorism Activity

Strategic Goal 3.1: Enable Appropriate Enhanced Investigation and Prosecution of Domestic Terrorism Crimes.

Strategic Goal 3.2: Assess Potential Legislative Reforms.

Strategic Goal 3.3: Ensure That Screening and Vetting Processes Consider the Full Range of Terrorism Threats.

(IV) **Pillar Four:** Confront Long-Term Contributions to Domestic Terrorism

Pillar Three is of particular interest in regard to this thesis. Its focus on enhanced investigations of crimes of domestic terrorism can be closely related to provisions under Title II: Enhanced Surveillance Procedures of the USA PATRIOT Act of 2001 which involve surveillance of terrorist activity. In addition, this report continually references the invaluable role that law

enforcement, especially on the Federal scale, plays in the success of counterterrorism initiatives in the United States. The NSC (2021) explains how the FBI is the lead federal law enforcement and intelligence agency that is tasked with investigating domestic and international terrorism and emphasizes that federal law enforcement agencies and investigators serve as a critical resource for countering domestic terrorism in the United States. This portion of the NSCDT supports statements made in the *National Strategy for Counterterrorism* (ODNI, 2018) which supports and emphasizes the notion of law enforcement officers and agencies as "frontline defenders" because they are the most influential and integral factor directly involved in the implementation of U.S. counterterrorism strategies. The concepts of technology, WMDs, radicalism/extremism, and domestic terrorism are linked together and discussed at length throughout the NSCDT; the United States government makes a clear and deliberate effort to highlight the negative implications of domestic terrorism on public health and national security. The National Strategy for Counterterrorism emphasizes the rise in domestic terror incidents in the United States as well as the subsequent increase in the number of deaths and violent acts committed by those terrorists against people and property (ODNI, 2018). Domestic terrorism poses a more significant threat to the homeland due to the dramatic rise in DVEs since 9/11 (DNI, 2022). Thus, governmental agencies and federal law enforcement are tasked with updating counterterrorism policies with regard to their surveillance of terrorist activity in and outside of the United States. The *National Strategy for Counterterrorism* explains the importance of increased intelligence and information-sharing amongst law enforcement agencies in ensuring that these entities are fully equipped to "…identify and act swiftly against terrorist activity" (NSC, 2021). While foreign/international terrorism was the focus of concern in the years following the September 11th terrorist attack, there has been a dramatic rise in instances of domestic terrorism. Radical and extremist beliefs

are the primary motivators behind domestic terrorists. Domestic terrorists are motivated by a wide variety of beliefs such as forms of "…violent extremism, such as racially motivated extremism, animal rights extremism, environmental extremism, sovereign citizen extremism, and militia extremism" (ODNI, 2018). One of the most recent and noteworthy examples of this phenomenon was the attack on the Capitol on January 6, 2021, by extremists who believed that the 2020 U.S. presidential election was rigged in favor of Joe Biden. Waves of rioters breached the doors of the United States Capitol in Washington, D.C. with the intention of overthrowing the government and reinstating Donald Trump as President. The anti-government sentiments of many of the attackers are an example of militia extremism. The FBI (2011) defines militia extremists as those individuals who "…believe that the Constitution grants citizens the power to take back the federal government by force or violence if they feel it's necessary." The *National Strategy for Countering Domestic Terrorism* has adopted a strategy to mitigate and reduce the rise in domestic terrorism that is both "persistent and evolving" and one that denounces and punishes domestic terrorists regardless of their specific beliefs or ideology motivating them to commit violent acts (NSC, 2021). The NSCDT is, ultimately, a modernized approach to counterterrorism strategies.

Strategic Framework for Countering Terrorism and Targeted Violence. The next item to evaluate in relation to surveillance as a counterterrorism tool for law enforcement is the Department of Homeland Security's *Strategic Framework for Countering Terrorism and Targeted Violence.* One method utilized in the surveillance of potential terrorist activity is technology that can screen individuals and detect terrorists "…attempting to travel to, or gain or maintain access to, the United States" (DHS, 2019). As we know from the horrific terrorist attacks on September 11, 2001, four airplanes were hijacked by a total of 19 terrorists, some of

which were able to bypass being selected by CAPPS (Computer Assisted Passenger Prescreening System); “Their selection affected only the handling of their checked bags, not their screening at the checkpoint” (9/11 Commission, 2004). Ultimately, post-9/11 fears of similar terrorist attacks were brewing across the nation. This fear was the catalyst in the creation of new surveillance provisions, specifically those outlined in Title II of the USA PATRIOT Act of 2001. The four goals listed and emphasized under the *Strategic Framework for Countering Terrorism and Targeted Violence* align with multiple ideas presented in the conceptual model at the conclusion of this Chapter. The topics of new counterterrorism strategies and efforts to strengthen national defense, which are listed in the model, can be related to each of the goals. For instance, the essence of goal 1 is to gain awareness and understanding of the phenomena that is the evolving threat of terrorism and targeted violence, as well as provide support to those involved in the efforts of protecting the homeland. The *Strategic Framework* emphasizes that goal 2 is intended to restrict terrorists from coming into the United States and reject the ability for them to take advantage of the Nation’s resources as well as its systems involved in trade, immigration, and domestic and international travel (DHS, 2019). Goal 3 is simplistic in nature in that it merely states the Department of Homeland Security’s intention to prevent terrorism and targeted violence, which was mentioned in goal 1. Finally, the purpose of goal 4 is to enhance the protections of United States critical infrastructure as well as strengthen community preparedness (DHS, 2019). On the other hand, the Strategic Framework for Countering Terrorism and Targeted Violence is also a key source that emphasizes how extremism and radicalism serve as the pillars of motivation behind many domestic terrorists. Hate crimes and acts of domestic terrorism are closely interrelated because the vast majority of domestic terrorists choose their targets based on personal factors like race, ethnicity, national origin, religion, sexual orientation, and gender

identity (DHS, 2019). The threat of domestic terrorist attacks plaguing the nation has drastically increased since 9/11; instances of domestic terrorism are becoming more prevalent than those of foreign/international origin (DHS, 2019). A simplified explanation for this occurrence is the rise in home-grown terrorists.

Homeland Security Twenty Years After 9/11: Addressing Evolving Threats. An increase in domestic terror-related incidents calls for a different approach to counterterrorism strategies in the United States. The emergence of radical and extremist beliefs has fueled domestic terrorism and caused it to be more of a threat than international terrorism. Domestic or "homegrown" terrorists pose a huge risk to the state of national security. Thus, federal law enforcement officers and investigators must be aware of this phenomenon in order to successfully implement and execute procedures that involve them monitoring and conducting surveillance of terrorist activity. A concern presented by Swalwell & Alagood (2021) highlights the increasing prevalence of domestic terror threats against the United States. Domestic terrorists are often motivated by violent, extremist beliefs. The concept of indoctrination is introduced and correlated to an increased prevalence in domestic extremism. The January 6th attack on the U.S. Capitol in 2021 is one of the most notable instances of extremism in modern-day domestic terrorism. *Homeland Security Twenty Years After 9/11: Addressing Evolving Threats* highlights domestic terror groups such as the Proud Boys and Oath Keepers, both of which exemplify the correlation between anti-government and white supremacist beliefs and ideologies. In addition, the authors emphasize the negative implications of violent domestic extremism on public health and safety. The notion of a convergence between similar beliefs amongst domestic extremists/terrorists is highlighted in the text and describes how this leads to insufficient and/or ineffective counterterrorism procedures. Swalwell & Alagood (2021) state, "Ideological

convergence makes intelligence and homeland security's counterterrorism mission difficult because 'it confuses counterterrorism defenses, eroding predictability and challenging law enforcement and intelligence categorizations.'"

Rethinking Terrorism and Counterterrorism Since 9/11. Hoffman (2002) highlights the extent of impact that Osama bin Laden and al Qaeda's attack on September 11, 2001, had on the implementation of counterterrorism efforts in the United States post-9/11. Hoffman (2002) details the uprising of al Qaeda and how bin Laden has functioned as a "terrorist CEO" throughout his deadly reign as leader of the organization. When the terrorist organization built by bin Laden executed their deadly attacks on 9/11, they permanently changed the way that Americans perceive terrorism and national security. The September 11, 2001, terrorist attacks targeted well known, prominent buildings and governmental institutions that stood to represent globalization and the prosperous stature of the American economy. The declaration of war by Osama bin Laden and his terrorist counterparts shocked the nation like never before. The author identifies four distinct types of operational techniques within al Qaeda: the professional cadre, the trained amateurs, the local walk-ins, and like-minded insurgents, guerrillas, and terrorists (Hoffman, 2002). The political and religious underpinnings of al Qaeda's attack on the United States were a stellar example of the extremist/radical beliefs held by certain terrorist groups. In fact, Hoffman (2002) argues that Osama bin Laden's impact on the United States is still seen in glimpses throughout American culture and society; "His effective melding of the strands of religious fervor, Muslim piety, and a profound sense of grievance into a powerful ideological force stands—however invidious and repugnant—as a towering accomplishment". The author stresses that bin Laden's attack on the United States on September 11, 2001, exposed the innate weaknesses borne to the preservation of national defense and homeland security. In addition,

9/11 permanently altered the way that Americans perceive the threat of terrorism against the U.S. Specifically, the author highlights how the impact of 9/11 exposed vulnerabilities in U.S. national security, subsequently resulting in a nationwide change in public attitude with regard to the fervor and will to counter and combat terrorism "…systematically, globally, and most importantly, without respite" (Hoffman, 2002). The events of 9/11 showcased the unfortunate situation in which the United States was wholly unprepared for an attack of such magnitude. Osama bin Laden and his al Qaeda counterparts were attempting to dismantle and disintegrate the previously held notions of peace and freedom that are supposed to be inherent to our democracy. Ultimately, Hoffman (2002) believes that a critical component of counterterrorism efforts is to adapt procedures that are as aggressive, if not more, than the enemy.

Re-imagining the Borders of US Security After 9/11: Securitisation, Risk, and the Creation of the Department of Homeland Security. The terrorist attacks on September 11th, 2001, resulted in a near-instantaneous restructuring of United States bureaucracy and homeland security policy. Mabee (2007) argues that the fear of another attack, like those on the World Trade Center and the Pentagon, and the resulting "War on Terror" by the Bush Administration, was the catalyst for establishing agencies and counterterrorism legislation aimed towards rebuilding and solidifying national defense strategies. The establishment of the Department of Homeland Security was one of the cornerstones of post-9/11 counterterrorism and anti-terrorism efforts. The formation of the DHS allowed America to establish an executive department comprised of multiple agencies that would oversee the goal of protecting the homeland. The DHS was formally created when President George W. Bush signed the Homeland Security Act of 2002 into law. The terrorist attacks on 9/11 and the 2001 anthrax attacks solidified the belief in both public and private sectors that a federal department capable of combatting terrorism was an

essential next step for the U.S. government to undertake. Not only did 2001 consist of the deadliest terrorist attack on U.S. soil when the World Trade Center, the Pentagon, and other governmental buildings were targeted by al Qaeda, but it also brought about the first bioterrorist attack on the U.S. in the 21st century (CCR, 2002). This bioterrorist attack involved the mailing of numerous letters covered in a powder, which ultimately ended up being anthrax spores, to various individuals working in media outlets, as well as postal workers, prominent politicians and governmental figures; twenty-two innocent people were infected with anthrax and five of them passed away due to severe health complications from the deadliest form of anthrax: inhalation/pulmonary (CCR, 2002). This solidified the need to establish some sort of governmental department that would be able to oversee the threats posed against homeland security in order to ensure the protection of our nation from any and all types of terrorism, and preserve our democracy in the meantime, was a clear and critical next step in the recovery from these events. The 107th Congress enacted the Homeland Security Act on November 25th, 2002, which was legislation that formally established the Department of Homeland Security. The intended purpose of the Homeland Security Act was, "To establish the Department of Homeland Security, and for other purposes" (Pub. L. 107-296, 2002). The establishment of the DHS along with the enactment of counterterrorism legislation, such as the USA PATRIOT Act of 2001, has resulted in public concerns regarding the government's influence on domestic freedoms, securities, and civil liberties; Mabee (2007) explains the growing issue of public confidence in government counterterrorism strategies when he highlights "'…the practical problems of sustaining civil liberties while facing the challenge of an active crisis of national security with no apparent end'" (Morgan, 2004, p. 7). The establishment of the Department of Homeland Security in November of 2002 was the turning point for the U.S. government with regard to sentiments

towards the threat of terrorism that persists. The mission or goal of the DHS involves providing for the security and safety of the American people, property, and sovereignty by securing the homeland, mitigating terrorism in the U.S., reducing the nation's vulnerabilities, minimizing the damage and destruction from attacks, and provide assistance in the recovery process after any terrorist attack (Swalwell & Alagood, 2021). The Department of Homeland Security's creation was a key factor in the federal government's efforts to implement more aggressive programs targeting terrorism. *Re-imagining the Borders of US Security after 9/11: Securitisation, Risk, and the Creation of the Department of Homeland Security* emphasizes the role that the September 11 attacks played in this restructuring of the United States government and its security bureaucracy with the intention of producing a safer nation that would be free from the threat of terrorism (Mabee, 2007). Exploring the policy implications surrounding border security post-9/11 and the subsequent effect that this catastrophic terrorist attack has had on national defense and U.S. counterterrorism strategies is of the utmost importance. Specifically, the author explains how the attacks on September 11th, 2001, was a turning point in the securitization process concerning terrorism and that it resulted in a newer and different culture of threat—one that necessitates unprecedented kinds of action, including emergency measures described by the securitization approach and the creation of new institutions focused on national security (Mabee, 2007).

Contemporary Policy Challenges in Protecting the Homeland. The policy implications of U.S. counterterrorism strategies are extensive. Homeland security can best be understood through interpretation of the Department of Homeland Security's goals which involves countering terrorism and homeland security threats, securing the borders as well as cyberspace and critical infrastructure, preserving the integrity of the nation, strengthening the security of the economy, enhance the preparedness and resilience of the United States government and its

people (DHS, 2019; Eller & Wandt, 2020). The establishment of counterterrorism protocol and procedures is supported through the creation of policies. Throughout *Contemporary Policy Challenges in Protecting the Homeland,* the authors define and relate four areas of homeland security policy "domain" to counterterrorism procedures. Those four areas involve funding, process, networking, and risk/risk management. A central argument is that each of these aspects of homeland security policy domain require additional clarification and/or significant editing. Eller & Wandt (2020) explain, "Federal policy and resource distribution decisions on homeland security activities are based squarely within the vision documents developed by DHS and in line with various DHS strategic goals." The authors emphasize how the 9/11 terrorist attacks were the catalyst in establishing legislation and policy surrounding homeland security; they explain that 9/11 was a turning point "...for the inception of a policy domain focused on homeland security, and with it came a body of research substantively concentrated on public policy addressing the unique challenges presented in the emerging policy domain" (Eller & Wandt, 2020). Some literature on homeland security is reviewed with the intention of explaining and emphasizing how the attacks committed on behalf of Osama bin Laden's terrorist counterparts, known as al Qaeda, led to an instantaneous restructuring of U.S. bureaucracy and policy with regard to counterterrorism strategies. The notion of the homeland security policy domain being riddled with complications is highlighted by the authors to a great extent. For instance, Eller & Wandt (2020) emphasize how the nature of homeland security policy is starkly different from any other policy domain considering the implications it has on public health and national safety. Trust issues arise amongst researchers and the public when analyzing the degree of power vested in officials who are directly involved in the preservation of homeland security. These trust issues

cause public confidence in government counterterrorism strategies to shift between optimistic and pessimistic mindsets.

The many faces of counterterrorism: an introduction. Analyzing the implications of U.S. counterterrorism policy can be accomplished by highlighting the impact that 9/11 had on the restructuring of such policy. The core argument to *The many faces of counterterrorism: an introduction* centers around the issue of terrorists identifying and subsequently exploiting weak areas of U.S. counterterrorism strategies. Sandler (2011) highlights two sides of counterterrorism efforts: proactive and defensive. Proactive efforts are offensive in nature and involve the government directly confronting terrorists and their counterparts. An example of proactive counterterrorism strategies includes targeting the resources, finances, safe havens, infrastructure, and/or sponsors that aid terrorists in their heinous attacks; defense counterterrorism measures consist of actions that "…harden targets, thereby making it more difficult and costly for the terrorists to attack successfully. Moreover, such measures also limit losses in the event of a successful attack…" (Sandler, 2011). Sandler (2011) utilizes twelve articles relevant to the topic of counterterrorism and national defense to provide a basis of understanding for the reader. A sort of literature review is conducted by Sandler (2011) in his effort to thoroughly inspect the vast, complex realm of U.S. counterterrorism policy and procedures. The author makes a recommendation for further research studies to be conducted by means of grouping proactive and defensive counterterrorism tools together, rather than isolating them and analyzing them individually. Sandler (2011) highlights the importance of combatting both domestic and transnational terrorism since they play equal parts in U.S. counterterrorism strategies and policies; "Effective policy must not only unite countries against transnational terrorist groups,

but also join authorities at different jurisdictional levels against domestic and transnational terrorist groups" (Sandler, 2011).

Understanding Public Confidence in Government to Prevent Terrorist Attacks. Baldwin et al. (2008) defines a prominent concern in the realm of counterterrorism: public confidence. This concept is referring to U.S. citizens as a whole and their perceptions and subjective assessments of the government and law enforcement agencies' ability to produce the intended result of counterterrorism efforts. The article begins by defining the prominent features of this concept. For example, the authors stress, "Public confidence has two components — an authority in which the confidence is placed and a subject to which the confidence refers" (Baldwin et al., 2008). Baldwin et al., (2008) conducted a study in which they employed research methodology that involved presenting a questionnaire to three groups. The purpose of this questionnaire was to assess the participants' confidence, or lack thereof, in governmental procedures that target terrorist activity. The goal of this overall study was to research the correlation between levels of public confidence and incidences of terrorism. In other words, the authors were primarily motivated to conduct this study in order to gain an understanding of the true impact of terrorist activity on public confidence. Assigning a numeric value to public confidence was an essential part of this study and its effort in planning to prevent and/or mitigate future terrorist attacks. The result of the study determined that the aggregate degree of confidence amongst the participants was low (Baldwin et al., 2008). The author highlights the fact that the Department of Homeland Security lists public confidence as a contributing factor to the impact of terrorist attacks. It is important to note the article's emphasis on the role of federal, state, and local law enforcement entities in the execution of U.S. counterterrorism strategies. Federal law enforcement officers and investigators must take public confidence into account with regard to their implementation of the

enhanced surveillance procedures listed under Title II of the USA PATRIOT Act of 2001. If public confidence is low, it is logical to assume that federal law enforcement's surveillance of terrorist activity will not be well-received by the general public, thus causing such surveillance strategies to be insufficient and/or ineffective with regard to monitoring electronic, wire, and oral communications that may be related to terrorism. The importance and relevance of public confidence to this research question and development of propositions is discussed further in Chapter 3.

The Dynamics of Terrorism and Counterterrorism: Understanding the Domestic Security Dilemma. This research delves into interrelated concepts such as counterterrorism, public confidence/opposition, and national (domestic) security. Field (2017) discusses the unintentional consequences of implementing counterterrorism protocol in the United States. One of the downsides that is perhaps the most impactful is growing public concerns of government oppression and invasions of personal privacy. The article emphasizes how counterterrorism efforts are struggling to stay afloat in this modern day and age considering the public's wavering concern about various counterterrorism strategies like the utilization of surveillance technology for the monitoring of potential terrorist activity. Ultimately, there is a large portion of the American population that disagrees with counterterrorism efforts like surveillance because they are worried about the legitimacy and effectiveness surrounding them. Public support is one of the most critical components in the successful implementation of such government initiatives. Field (2017) introduces and explains the concepts of domestic and international security dilemmas in relation to counterterrorism policy in the U.S. Essentially, the 'security dilemma' is a term that can be helpful when assessing the relationship between counterterrorism strategies and resistance from the public. The article explains that this dilemma is the consequence that results from the

enhancement of governmental authority unintentionally making people more concerned about government oppression and the violation of civil liberties. This exemplifies a security dilemma, because there is "…seemingly no acceptable government response to terrorist threats" (Field, 2017). The author argues that public opposition to governmental strategies breeds ineffective policies on the matter of counterterrorism and that such policies intended to enhance security have a "counterproductive and paradoxical effect…undermin[ing] attempts to make people feel safe from terrorism" (Field, 2017). Field (2017) explained how the security dilemma has led to certain post-9/11 counterterrorism strategies being short lived; "Some of the most high-profile intelligence practices that were abandoned included extraordinary rendition, enhanced interrogation, and the 'Total Information Awareness' program for domestic surveillance." Field (2017) emphasizes the vital role that the American population plays in the execution and usage of government counterterrorism procedures and tools. The complex, multifaceted nature of counterterrorism requires a great deal of cooperation on behalf of the general public. With regard to federal law enforcement using surveillance technology as a counterterrorism strategy, we see a similar issue arise. Surveillance as a counterterrorism tool is innately contradictory; it aims to mitigate and prevent acts of terrorism from occurring, but the process itself is inherently controversial because the surveillance technology often involves a substantial degree of intrusion, especially into the private lives of innocent American citizens.

Surveillance As Law. This article pursues topics like surveillance, 9/11, and counterterrorism efforts in the United States. A focus of this paper is the outbreak of an information state, which Cockfield (2011) describes as an environment of heightened concern regarding terrorism in which the role of the federal government transitions towards increasing the "…capacity for, and policy push towards, enhanced surveillance". The author emphasizes,

"The new policies rely on collecting information flows (often in real or near-real time) to detect activity that may threaten the state – they access ongoing streams of personal information such as GPS signals from cell phones that track an individual's movement. At times, this information is fed automatically into predictive software programs that may trigger crime and terrorism investigations" (Cockfield, 2011). Cockfield (2011) highlights the critical role that law enforcement officers and investigators, who are part of the information state, play in the collection, interception, and dissemination of information that was gathered by surveillance tools and devices; "More recent technology developments — Forward Looking Infrared Radar searchers, Internet Service Provider (ISP) and satellite monitoring, cell phone geotagging and so on…permit the police to conduct their investigations without the knowledge of the suspects". Ultimately, the intention behind this paper was to reinforce the increased prevalence of surveillance procedures being utilized in the enforcement of law, however, Cockfield (2011) makes a concerted effort to point out the contradictory nature of such operations; he emphasizes that there is an underlying implication of corruption surrounding these newer surveillance devices and methods.

The Fear of Counterterrorism: Surveillance and Civil Liberties Since 9/11. Deflem & McDonough (2015) emphasizes the growing concerns of potentially illegal, unethical, and/or unconstitutional access of the private and personal information of American citizens by the United States government. Deflem & McDonough (2015) explain that a 2013 study showed that approximately 53% of United States citizens do not approve of surveillance programs being conducted by the federal government. The authors argue that the increase in sophisticated surveillance technology being utilized by the government and, federal law enforcement especially, is breeding a culture afraid and untrusting of the government. They explain that this

phenomenon has been exacerbated by the haphazard enactment of anti-terrorism/counterterrorism legislation post-9/11. Specifically, the USA PATRIOT Act of 2001 is the "…most prominent and commonly scrutinized source of the formal expansion of investigative powers in the United States" Deflem & McDonough, 2015). Deflem and McDonough (2015) emphasize the evolving and emerging notion of counterterrorism initiatives being inherently unconstitutional as they present major threats to civil liberties such as freedom of privacy and speech. Civil liberties are freedoms bestowed upon citizens of the United States which are guaranteed by the U.S. Constitution and emphasized in the First Amendment. The authors point out that, in this modern day and age, there exists an evolving culture that is driven by a heightened perception of sensitivity with regard to civil liberties and the perceived attacks on them by governmental counterterrorism initiatives; "Fear justifies and motivates the use of surveillance, while the expansion of surveillance produces a cultural fear of its capabilities and consequences" (Deflem & McDonough, 2015). This fear is concerning when assessing the effectiveness of counterterrorism efforts in the United States because it hinders the ability of the government and federal law enforcement to carry out such procedures that are deemed too invasive by the public. The research conducted in this study analyzes the Office of the Inspector General's semi-annual report on claims of civil liberties being violated by employees of the Department of Homeland Security. The authors concluded that the number of claims exceeds the number of proven violations. The main concluding point is that this is the result of an emerging culture of apprehension and a manifestation of unique sensitivities with regard to civil liberties and surveillance technology/strategies.

NSA Surveillance Since 9/11 and the Human Right to Privacy. Groups such as the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), and especially the

National Security Agency (NSA) have been involved in the amassing of data about American citizens under the aim of preventing terrorist attacks from occurring in the future (Sinha, 2014). The organizations are all involved in the surveillance of terrorist activity. For instance, the NSA possesses collection systems which are utilized to intercept, track, and store almost 2 billion e-mails, text messages, phone calls, and various other means of communication (Cockfield, 2011). *NSA Surveillance Since 9/11 and the Human Right to Privacy* discusses the impact of the NSA 'program' on the various surveillance strategies executed by the United States government and federal law enforcement. Sinha (2014) provides insightful context in regard to this program when he referenced a 2005 *New York Times* publication of the newfound clearance authorized by President George W. Bush in a "secret 2002 executive order" which allowed the National Security Agency to engage in the direct surveillance (i.e., 'eavesdrop') and collection of domestic and private cellphone calls and e-mails without having a warrant(s) approved by the courts. When President George W. Bush signed the USA PATRIOT Act of 2001 into law on October 26, 2001, one of the purposes of this landmark piece of counterterrorism legislation was to change, or amend, FISA. The USA PATRIOT Act of 2001 made revisions to the Foreign Intelligence Surveillance Act which subsequently helped facilitate more invasive government surveillance efforts. These revisions authorized federal law enforcement agents to apply for a court order requesting a roving warrant in an investigation related to terrorism and national security. Sinha (2014) highlights one specific section of the USA PATRIOT Act of 2001 as it relates to roving warrants and, ultimately, federal law enforcement's surveillance of terrorist activity. The provision under Title II: Enhanced Surveillance Procedures amended the Foreign Intelligence Surveillance Act of 1978 by authorizing federal law enforcement to implement roving surveillance for the purpose of obtaining foreign intelligence information. While this is

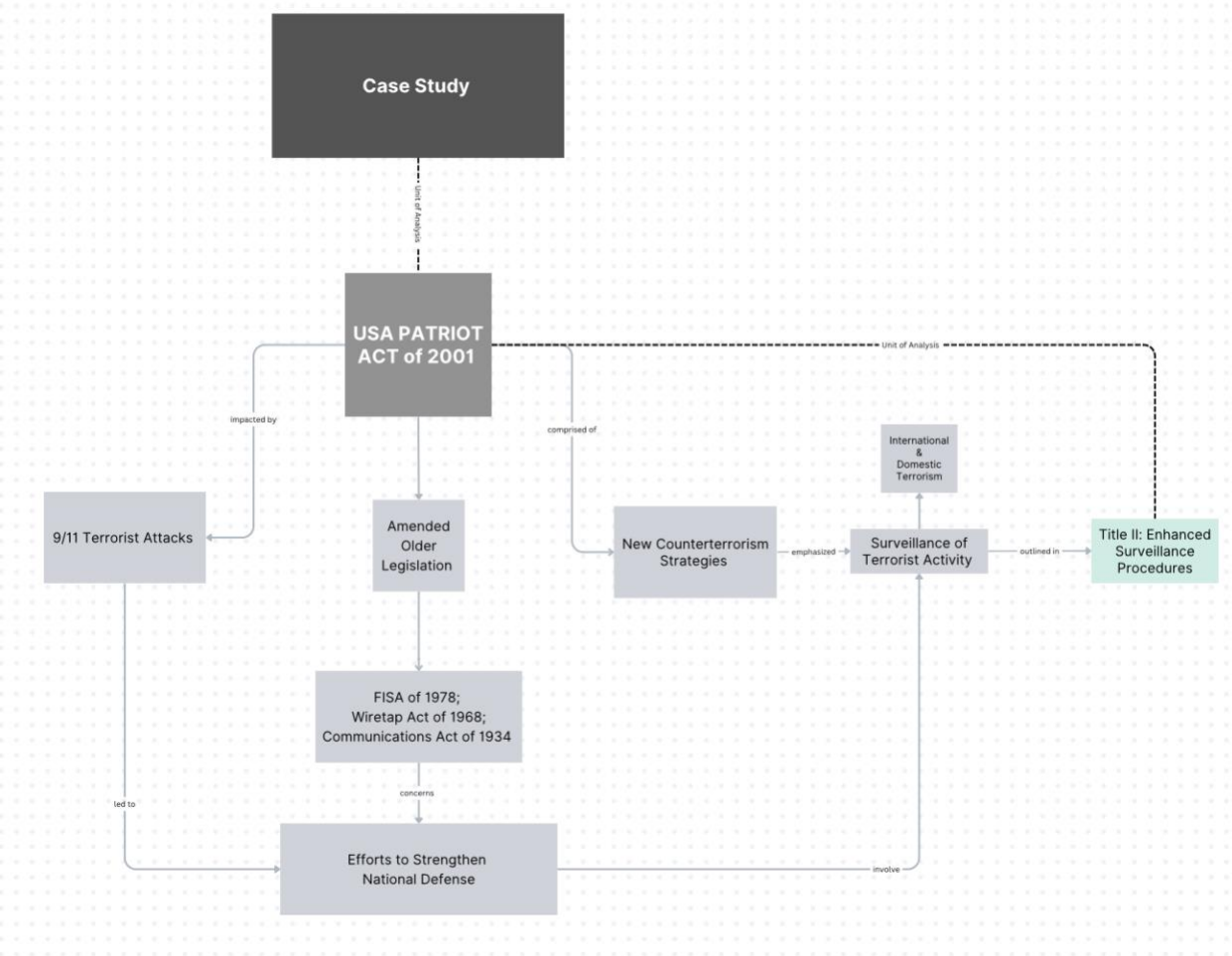
not a new law enforcement technique, the legislation expanded the ability for law enforcement to gather information on a wider range of terrorist-related crimes and criminal activity involving chemical-weapons offenses, the use of WMDs (weapons of mass destruction), the murder of American citizens abroad, and terrorism financing, according to the United States Department of Justice (2023).

Law Enforcement's Role in US Counterterrorism Strategy. Brooks (2010) extensively reviews the various measures that U.S. law enforcement takes in the counterterrorism strategy which the United States has adopted. The author, Bret E. Brooks, has life-long experience in the field of policing—as a state law enforcement officer and a Captain in the United States Army, Brooks's insight on the role of police in the United States's overarching counterterrorism strategy is of immeasurable value to the expansion of the theory underlying this thesis. Law enforcement agencies, investigators, and officers have become drastically more involved in counterterrorism efforts since 9/11. Brooks (2010) explained that "…counterterrorism measures being used by law enforcement agencies include technical surveillance of suspects, interviews, interrogations, proactive threat assessments, and other related procedures…This coincides with the four pillars of the US National Strategy for defeating, denying, diminishing and defending against terrorists" (Brooks, 2010). Brooks emphasizes his belief that police officers are the most adequately equipped, mentally and physically, to execute counterterrorism procedures and strategies; he cites the keen investigatory skills that law enforcement possess and hone on a daily basis. Brooks points out that law enforcement can only be successful in their duties if they are given the proper tools and resources necessary to counter terrorism. He believes that the government has a responsibility to supply police agencies at federal, state, and local levels with adequate provisions to execute U.S. counterterrorism strategies. Brooks (2010) states that such provisions

would include funding, training, equipment, and personnel, which would be disseminated under the direction of Congress for the purpose of advancing counterterrorism measures in the United States. Finally, Brooks (2010) concludes the article by highlighting how interdepartmental intelligence and information sharing amongst law enforcement agencies is a critical asset to the success of counterterrorism operations. The mobilization of law enforcement at both foreign and domestic levels is critical in the effective implementation of counterterrorism procedures in the United States.

The USA PATRIOT Act of 2001's speedy enactment only one-month post-9/11 was controversial. The research question guiding this thesis delves into the way that the USA PATRIOT Act of 2001, a landmark piece of U.S. counterterrorism legislation, has impacted the way that federal law enforcement conducts surveillance of terrorist activity in the United States. Title II of the USA PATRIOT Act of 2001 specifically expands the scope of authorities for federal law enforcement officers and investigators with regard to engaging in the interception, collection, and sharing/dissemination of information gathered from electronic, wire, and/or oral communications that are related to terrorism and computer fraud and abuse offenses. American law enforcement plays one of the most influential parts in U.S. counterterrorism efforts. This profound piece of legislation has facilitated easier investigatory processes for law enforcement officers in the context of counterterrorism strategies.

Conceptual Model. The following image is a conceptual model which highlights some of the core components of this thesis:



This Chapter provided an exhaustive literature review of 15 texts ranging from government publications to scholarly research articles. The goal of this was to analyze literature on topics including, but not limited to, international and domestic terrorism, counterterrorism, surveillance, the USA PATRIOT Act of 2001, 9/11, homeland security/national defense, and radicalism/extremism. The purpose of this literature review was to provide the reader with insight into the concepts that are discussed at length throughout the remainder of this work and examine the conclusions that previous researchers have come to regarding these topics. The next Chapter explains the methodology and research design of this thesis and case study analysis.

Chapter 3 – Methodology

The information within Chapter 2 was gathered by retrieving articles published through scholarly journals and evaluating their value to this thesis. The Academic Search Complete (EBSCOhost) online research database available through Youngstown State University's Maag Library serves as the central source of articles that are analyzed throughout this literature review. This is a comprehensive scholarly, multi-disciplinary full-text database with thousands of peer-reviewed journals. Criteria for selection was exclusively based on peer reviewed sources that were published post-9/11. More specifically, I selected articles that were published between the years 2002 and 2023.

The methodology utilized for this thesis consists of an explanatory, single-case study. Simply put, "…the case study as a research strategy comprises an all-encompassing method—covering the logic of design, data collection techniques, and specific approaches to data analysis" (Yin, 2003). Essentially, "case study" is an umbrella term that encompasses three specific techniques that may be applied in case study analysis. An explanatory case study is categorized by the presence of a "how" or "why" question which serves as the foundation for the analysis. This specific type of research methodology involves building an explanation about a particular case reflects some significant theoretical proposition. According to *Case Study Research: Design and Methods,* the extensive nature of explanation building involves creating an initial theoretical statement or proposition about a policy or social behavior and then comparing the findings from an initial case against that proposition (Yin, 2003). He also identifies an iterative nature behind explanation building for explanatory case study analyses; "…the case study evidence is examined, theoretical propositions are revised, and the evidence is examined once again from a new perspective, in this iterative mode" (Yin, 2003). Yin (2003) describes how a theoretical

proposition is simply a hypothetical story or answer to the "how" or "why" research question that is guiding a case study analysis. For an explanatory case study analysis, such propositions are a critical part of the research methodology, however, there is an emphasis on how the subtle, yet bold, process of explanation building is closely related to the process of "refining a set of ideas, in which an important aspect is again to entertain other *plausible or rival explanations*" (Yin, 2003).

The very first step in the path to conduct a case study analysis "…begins with a thorough literature review and the careful and thorough posing of research questions or objectives" (Yin, 2014). The establishment of initial and final theoretical propositions serves as the general analytic strategy[3] for this case study. Relying on such propositions and their explanations is vital to this type of analysis, however, the inclusion of rival explanations is equally as important to ensure that the final theoretical propositions are fully justified (Baškarada, 2013). A rival explanation, in essence, is a contradictory or 'rival' proposition that presents an opposing theory to the original theoretical proposition/hypothesis. Yin (2003) justifies that rival explanations are a critical component of case study analysis in addition to relying on theoretical propositions because they help the researcher establish confidence in the study's findings. Simply put, a basic or 'direct rival' would state that the observed outcome of a study was the result of another variable or influence besides the one presented in the theoretical proposition.

The research question guiding this thesis is the following: How has the USA PATRIOT Act of 2001 impacted the way that federal law enforcement conducts surveillance of terrorist activity in the United States? Determining the relationship between Title II of the USA PATRIOT Act of 2001 and federal law enforcement's implementation of surveillance technology with the

[3] Yin. R.K. (2003). Case Study Research: Design and Methods. Third Edition, p. 111-112

intention of monitoring, mitigating, and preventing terrorist activity is essential to the development of the later chapters in this thesis. Assessing the causal link between the execution of the surveillance of terrorist activity and Title II of the USA PATRIOT Act of 2001 by means of a "how" question is the reason an explanatory case study is chosen for the methodology of this thesis. An explanatory case study involves causal/explanatory research which identifies the extent and nature of a cause-and-effect relationship between two or more variables. In this thesis, the 'variables' can be described as federal law enforcement's surveillance of terrorism and the USA PATRIOT Act of 2001, specifically Title II under this Act. Although the nature of case study analyses proves to be mostly non-experimental, this does not mean that the research is non-quantitative. In fact, Yin (2003) describes the importance of reporting and analyzing experimental and/or survey data and relating this information to decisions and other characteristics of the report in order to illuminate a decision, policy, or practice. For this thesis, quantitative data and statistics are drawn from previous research articles and incorporated throughout this thesis to support the theory that the USA PATRIOT Act of 2001 was a groundbreaking piece of counterterrorism legislation that impacted federal law enforcement's surveillance of terrorist acts in or against the United States by authorizing them to use surveillance technology in their investigations.

As Yin (2003) recommends, the formation of theoretical propositions and subsequent rival explanations serves as the backbone of this case study analysis of the USA PATRIOT Act of 2001. For this thesis, an initial theoretical proposition, explanation, and rival explanation are developed; after the case study analysis within Chapter 4, a final theoretical proposition, explanation, and rival explanation are established. The research question that is at the core of this thesis aims to evaluate how the enactment of the USA PATRIOT Act of 2001, specifically the

provisions underlined in Title II: Enhanced Surveillance Procedures, have affected the way U.S. federal law enforcement conducts surveillance of terrorist activity. Surveillance procedures and technology used by federal law enforcement entities are designed and engineered to allow these entities to monitor various forms of communications with the goal of tracking and pinpointing terrorist activity.

The *initial theoretical proposition* guiding this thesis is the following: The enactment of the USA PATRIOT Act of 2001 has made it easier for federal law enforcement agencies, officers, and investigators to conduct surveillance in the United States and target and eliminate terrorist threats by amending existing legislation to enhance and expand their authorization to use electronic surveillance technology for the purpose of monitoring and tracking terrorists and their crimes. Title II: Enhanced Surveillance Procedures of the USA PATRIOT Act of 2001 strengthens United States counterterrorism strategies through its amending of legislation such as the Foreign Intelligence Surveillance Act of 1978, which established broad authorities for federal law enforcement's use of surveillance tools in their terrorism investigations. The *theory* being developed in this thesis explains that the USA PATRIOT Act of 2001 was a groundbreaking piece of counterterrorism legislation which heavily affected federal law enforcement's surveillance of terrorist acts in or against the United States by expanding preexisting authorizations under FISA in order to permit them to use enhanced surveillance technology and procedures in their terrorism investigations.

Despite the USA PATRIOT Act of 2001's enhancement of counterterrorism investigatory tools utilized by federal law enforcement, a low level of public confidence in governmental entities' ability to prevent terrorism has been observed post-9/11.[4] A *rival explanation* to the

[4] Baldwin et al. (2008) p. 16

initial theoretical proposition is as follows: Title II's impact on federal law enforcement's authorities related to their now expanded use of surveillance procedures and sophisticated surveillance technology for the purpose of monitoring terrorist activity has produced substantial backlash in the public eye due to a widely held perception of the invasion of privacy and, ultimately, a violation of the civil liberties bestowed upon every American citizen. Although Title II: Enhanced Surveillance Procedures under the USA PATRIOT Act of 2001 enhanced federal law enforcement's counterterrorism strategies and investigations, it cultivated a culture of government resistance by producing deeply rooted fears that the government is violating the First, Fourth, and Fifth Amendments to the United States Constitution by illegally monitoring and obtaining personal information and communications from innocent Americans. [5]

Yin (2003) highlights the importance of testing your case study analysis to ensure high-quality research has been conducted. These tests are an important part of the case study methodology. Four such tests exist to guarantee that the research being conducted for the case study analysis is both reliable and valid: construct validity, internal validity, external validity, and reliability. Tactics for accomplishing these tests occur throughout the entire thesis and involve the utilization of multiple sources of evidence and key informants (i.e., my thesis committee members) to review a draft of my case study report in order to establish construct validity; the building of explanations, addressing of rival explanations required to establish internal validity; the use of theory in single-case studies to establish external validity, and the use of case study protocol to establish reliability (Yin, 2003). To the best of my ability, I executed these tactics to test my research's reliability and validity. I break down the specific techniques I utilized for establishing reliability and validity across this thesis:

[5] Deflem & McDonough. (2015); DOJ. (2004).

(1) *Construct Validity:* As apparent in Chapter 2, a wide array of sources were used to obtain evidence and build my literature review. From scholarly articles to pieces of legislation and government strategy publications, it is no doubt that multiple sources of evidence and information were accessed and utilized in this thesis for the purpose of reviewing, analyzing, and clarifying literature surrounding the USA PATRIOT Act of 2001, federal law enforcement, terrorism, and surveillance. The other tactic I employed was having key informants review a draft of this thesis/case study report. Yin (2003) emphasized that this formal review of case study drafts is favorable and a "validating procedure," as it results in a higher-quality case study analysis by enhancing and increasing its construct;[6] my thesis has accomplished this through the formal defense of the proposal and the final version which were accompanied by the composition of numerous drafts that were reviewed by external sources—my thesis advisor and committee members.

(2) *Internal Validity:* Pattern-matching involves developing and addressing rival explanations which is the other side of a theoretical proposition in that the rival explanation would explain an outcome that is the direct opposite or "rival" of the theoretical proposition. Explanation building is a tactic for testing for internal validity. Similar to pattern-matching, Yin (2003) explains that this tactic involves examining the information and evidence, creating theoretical propositions, and revising those propositions in order to build an explanation about the case; the main element of explanation building is the analysis of causal links about a phenomenon which, in this thesis, is the USA PATRIOT Act of 2001's impact on federal law

[6] Yin, R.K. (2003) Case Study Research Design and Methods. Third Edition, pp. 159-161

enforcement's surveillance of terrorist activity. The creation and revision of my theoretical propositions and explanations begins in this Chapter and develops throughout the remainder of this thesis and case study analysis.

(3) *External Validity*: Yin (2014) explains that external validity is concerned with analytic generalization—the role that theory plays in generalizing the lessons learned from a case study analysis.[7] In order to establish external validity, it is helpful to pose a "how" or "why" research question. For my case study analysis, the theory can be stripped down and generalized to focus solely on the USA PATRIOT Act of 2001's impact on surveillance. Future researchers could apply the findings of this case study to new situations (i.e., how surveillance of American citizens was impacted versus the surveillance of terrorists).

(4) *Reliability*: Reliability is established through the documentation of case study protocol which is a tactic that clarifies the procedure taken in the analysis for the purpose of allowing a future researcher to repeat the same study and arrive at the same conclusions. The case study protocol utilized for this thesis is simplified in this Chapter.

Case Study Protocol

Step 1 – Decide a topic worthy of a case study analysis. Determine the type of case study analysis to be conducted (explanatory), the unit of analysis (Title II of the USA PATRIOT Act of 2001) and then formulate a research question to guide the thesis. [Completed in Chapter 1]

[7] Yin, R.K. (2014). Case Study Research, p. 40

Step 2 - Gather sources and conduct a literature review. [Completed in Chapter 2]

Step 3 – Develop an initial theoretical proposition and explanations based upon the initial research. [Completed in Chapter 3]

Step 4 – Link the unit analysis to the initial theoretical proposition, then develop the final theoretical proposition and explanations based on the findings. [Completed in Chapter 4]

This Chapter highlighted my procedures involved in conducting this case study, which have satisfied Yin's description of the technical components involved with executing this unique type of qualitative research analysis.[8] In the next Chapter, I present my findings relative to my research question and develop the final theoretical proposition and explanations. Chapter 4 involves two parts. Part I summarizes and analyzes each of the seventeen sections under Title II relevant to the research question. Part II relates those sections to the theoretical propositions and explanations.

Chapter 4 – Results

The USA PATRIOT Act of 2001 was passed by Congress on October 26, 2001. The following day, President George W. Bush signed this landmark piece of legislation, formally declaring it law of the United States. The title stands for *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.* Overall, the Act consists of ten titles that explicitly outline newfound protocol in countering terrorist activity. Title II: Enhanced Surveillance Procedures is the portion of the USA PATRIOT Act of 2001 that directly states new provisions for the monitoring and surveillance of concrete acts of terrorism or

[8] Yin, (2003); Yin, (2014).

potential acts of terrorism. Title II also outlines new authorities for federal law enforcement agencies and individuals, the goal of which is to facilitate smoother, yet more sophisticated, counterterrorism strategies. Federal law enforcement officers and investigators play the most important role in counterterrorism strategies since they are directly involved in the interception, collection, dissemination, and analysis of information that was gathered by surveillance technology and the nature of which relates to terrorism and/or crimes against the United States. Surveillance, in the context of this thesis, is a useful tool that federal law enforcement and other governmental entities can use to monitor and observe an individual under the scope of an investigation with the ultimate goal of preventing, mitigating, and defeating terrorism. As mentioned in Chapter 1, a significant purpose of the USA PATRIOT Act of 2001 is to facilitate intelligence-sharing amongst federal law enforcement agencies and government entities by "…enhanc[ing] law enforcement investigatory tools" (Pub. L. 107-56 2001). This thesis critically analyzes Title II of the USA PATRIOT Act of 2001 and examine its alleged purpose, as well as the effect that this title has had on federal law enforcement's implementation of surveillance procedures that targets and monitors all terrorist activity.

Part I. Summary and Analysis of Sections Under the USA PATRIOT Act of 2001 that Relate to Law Enforcement and/or Surveillance

Sec. 201. Authority to Intercept Wire, Oral, and Electronic Communications Relating to Terrorism.
Sec. 202. Authority to Intercept Wire, Oral, and Electronic Communications Relating to Computer Fraud and Abuse Offenses.

The first two sections under Title II: Enhanced Surveillance Procedures of the USA PATRIOT Act of 2001 amends § 2516 of Title 18 of the United States Code. 18 U.S.C. 2516 is

titled “Authorization for the interception of wire, oral, or electronic communications.” Under § 201 and 202 of the USA PATRIOT Act of 2001, the following authorities have been established for federal law enforcement: the authority to intercept wire, oral, and electronic communications relating to terrorism and computer fraud/abuse offenses. The logical reason for establishing these authorities is to enhance federal law enforcement’s terrorism-related investigations as well as facilitate the monitoring of individual and/or group engagement in terrorist activity. More specifically, § 201 amends 18 U.S.C. § 2516(1) by inserting an additional paragraph that expands the list of criminal violations and offenses investigated by federal law enforcement in their interception of wire or oral communications, as authorized by the application for such interception designated by any of the entities underlined in § 2516(1). § 201 is authorizing law enforcement to intercept such communications on the basis that the interception provides or may provide evidence of the following: any criminal violation of sections 229 (chemical weapons), 2332 (criminal penalties), 2332a (use of weapons of mass destruction), 2332b (acts of terrorism transcending national boundaries), 2332d (financial transactions), 2339A (providing material support to terrorists), or 2339B (providing material support or resources to designated foreign terrorist organizations) under Title 18 of the United States Code. § 202 amends 18 U.S.C. § 2516(1)(c) to include, under the seemingly endless list of punishable acts, offenses relating to § 1341 “Frauds and swindles” (relating to mail fraud), which is a felony violation of § 1030 “Fraud and related activity in connection with computers” (relating to computer fraud and abuse). Prior to the USA PATRIOT Act of 2001’s enactment, it was harder for federal law enforcement to eliminate terrorist threats because they could not use wiretaps for surveillance purposes to investigate these crimes (DOJ, 2023).

There are three distinct groups of individuals involved in § 201 and 202 under Title II: Enhanced Surveillance Procedures. The first group consists of the Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General, and the Deputy Assistant Attorney General. These entities exist within the Criminal Division or National Security Division that has been uniquely designated by the Attorney General. *An individual falling under any one of those titles may authorize an application to a federal judge that requests an order specifically approving the interception of wire, oral, and/or electronic communications by the FBI or other federal agency.*

The second group involves the principal prosecuting attorney of any State or the principal prosecuting attorney of any political subdivision thereof. *This person may apply to a state court judge for an order that would authorize or approve the interception of wire, oral, or electronic communications by investigative or law enforcement officers.*

The third and final group that possesses the authorities defined under Title II of the USA PATRIOT Act of 2001 consists of *any* attorney for the federal government. *Specifically, this individual is authorized to apply to a federal judge for an order that would authorize and/or approve the interception of electronic communications by an investigative or law enforcement officer.* It should be noted that the approval may only be given in the scenario where such interception would provide adequate evidence/may provide adequate evidence of any federal felony being committed.

In simpler terms, these sections expanded the range of terrorism and computer fraud/abuse crimes that federal law enforcement is authorized to investigate with electronic surveillance. The scope of federal law enforcement's surveillance of terrorism in the United States was expanded to include offenses related to the use of chemical weapons and weapons of

mass destruction,[9] the violation of criminal penalties,[10] terrorism acts in foreign countries,[11] the providing of resources, material, or financial support to foreign operations,[12] and the engagement of financial transactions with the government of a country that supports international terrorism,[13] This was done under the belief that acts of terrorism transcend the strict boundaries established by provisions in the Foreign Intelligence Surveillance Act of 1978.

Sec. 203. Authority to Share Criminal Investigative Information.

The establishment of § 203 under Title II: Enhanced Surveillance Procedures outlines and emphasizes newfound authorities for federal law enforcement and investigative officers. The authorities enable these entities: (a) to engage in the sharing of grand jury information; (b) to share electronic, wire, and oral interception information; and (c) to receive foreign intelligence information that will assist in the official duties of the federal officer/investigator(s). § 203 (a) Authority to Share Grand Jury Information under Title II is specifically amending Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure (FRCP), which defined the exceptions to the recording and disclosure of grand jury proceedings and explained how any attorney for the government may disclose any grand jury matter to another federal grand jury (18 U.S.C. App Fed R Crim P). Now, § 203(a)(1) under Title II amended this provision of the FRCP to expand the scope of disclosure of sensitive information that would have otherwise been prohibited, especially if it relates to foreign intelligence or counterintelligence, or foreign intelligence information (Pub. L. 107-56, 2001). In § 203 (b) Authority to Share Electronic, Wire, and Oral

[9] 18 U.S.C. § 229, 2332a
[11] 18 U.S.C. § 2332
[11] 18 U.S.C. § 2332B
[12] 18 U.S.C. § 2339A, 2339B
[13] 18 U.S.C. § 2332d

Interception Information, 18 U.S.C. § 2517 (Authorization for disclosure and use of intercepted wire, oral, or electronic communications) is amended to expand the abilities of federal law enforcement entities to disclose such information to any other federal law enforcement entity, intelligence, protective, immigration, national defense, or national security officer as long as the information relates to foreign intelligence or counterintelligence, or foreign intelligence information (Pub. L. No. 107-56 2001). 18 U.S.C. § 2517 falls under Chapter 119 — WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS of the Cybercrime Laws of the United States published in 2006. § 203(b)(1) under Title II states that any federal enforcement officer/investigator or federal attorney who has obtained information and or data originating from wire, oral, and/or electronic communications is authorized to share that information with "…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…or foreign intelligence information" (Pub. L. 107–55 2001). § 203(d) Foreign Intelligence Information states that it is lawful for foreign intelligence, counterintelligence, or foreign intelligence information that is obtained from a criminal investigation to be disclosed/shared with *any* federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist that official in the execution and performance of his duties (Pub. L. 107-56, 2001). After the enactment of the USA PATRIOT Act of 2001, disclosure of grand jury matters that was otherwise prohibited is now allowed to be disclosed to federal law enforcement and government entities if they involve foreign intelligence or counterintelligence or foreign intelligence information.

Sec. 206. Roving Surveillance Authority Under the Foreign Intelligence Surveillance Act of 1978.

§ 206 amends §105(c)(2)(B) under FISA. Specifically, § 206 inserts the following phrase: ", 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 "specific person" (Pub. L. 107-56 2001). In other words, § 206 is amending FISA to allow for "roving" warrants that apply to any and all phones/means of communication that are used or believed to have been used by an individual, rather than applying the wiretap to a specific phone number (Sinha, 2014). The DOJ (2023) explained that § 206 allows the Foreign Intelligence Surveillance Court (FISC) to authorize warrant(s) for "roving surveillance" when the court determines that the actions taken by the target may potentially thwart/inhibit the surveillance of their criminal/terrorist activities. The role of the FISC is to review federal law enforcement's applications for orders requesting the use of FISA surveillance (physical searches, electronic surveillance, roving warrants/wiretaps, pen registers and trap and trace devices) in terrorism investigations for the purpose of obtaining foreign intelligence (FISC, 2023). § 206 is important for federal law enforcement because it allows them to utilize "roving wiretaps" in investigations that involve matters of national security (DOJ, 2023). A "roving wiretap" is different from a normal wiretap that would target a specific phone or electronic device in that it would apply to the individual themselves and not just the device they are using for communication purposes (DOJ, 2023). The concept of "roving" warrants and wiretaps is not new—prior to 9/11, law enforcement used these options in their investigations into various crimes; however, § 206 expands this ability to allow federal law enforcement to use such "roving" surveillance efforts in their investigations into terrorism and threats against national security (DOJ, 2023).

Sec. 207. Duration of FISA Surveillance of Non-United States Persons Who Are Agents of a Foreign Power.

Under this section, four amendments are made to the Foreign Intelligence Surveillance Act of 1978. Two amendments extended the limits on the duration of time allowed for federal law enforcement to conduct surveillance as well as the duration of a physical search—the third amendment made involves extending the surveillance order under FISA while the last one expands the kind of individual that is targeted by the physical search.

The exact changes made under § 207 in the USA PATRIOT Act of 2001 consist of the following:

I. *§ 207(a)(1) [Duration of Surveillance] amends § 105(e)(1) of FISA*: An order for surveillance targeting an agent of foreign power may be for the period of time specified in the application for the order of surveillance targeting an agent of a foreign power that is a non-U.S. person, or for 120 days — whichever is less

II. *§ 207(a)(2) [Duration of Physical Search] amends § 304(d)(1) of FISA:* The duration of an order for a physical search targeting an agent of a foreign power that is a United States person may be for the period of time necessary to achieve the intended purpose of the search, or for 90 days — whichever is less. In addition, the duration of an order for a physical search targeting an agent of a foreign power that is a non-United States person may be for the period of time specified in the application, or for 120 days — whichever is less.

III. *§ 207(b)(1) [Extension in General] amends § 105(d)(2) of FISA:* The extension for a surveillance targeting an agent of a foreign power may be for a period not to exceed one year.

IV. *§ 207(b)(2) [Extension, Defined Term] amends § 304(d)(2) of FISA:* An extension of an order for a physical search targeted against a foreign power "or against an agent of a foreign power as defined in section 101(b)(1)(A)" may be for a period not to exceed one year (Pub. L. 107-56, 2001).

Prior to the enactment of the USA PATRIOT Act of 2001, the duration of FISA surveillance and search orders was 45 days instead of 90.

Sec. 209. Seizure of Voice-mail Messages Pursuant to Warrants.

§ 209 amends the definition of wire communication that was established under the Wiretap Act of 1968. Section 209 of Title II amended 18 U.S.C. § 2510(1) and the definition of electronic communications system under § 2501(14). This provision under the USA PATRIOT Act of 2001 also amended § 2703(a) and § 2703(b) of Title 18 of the United States Code. § 209 strikes the phrase "contents of an electronic" and changes it to "contents of a wire or electronic" anywhere it is mentioned. The inclusion of the term 'wire' is emphasized in this provision with the intention of expanding the scope of information to which a governmental entity, such as federal law enforcement, may require providers of electronic communication services and/or remote computing services to disclose the contents of wire and electronic communications in electronic storage or in a remote computing service (LII, 2023). The DOJ (2023) explains that § 209 facilitates federal law enforcement's investigations by allowing them to obtain voice-mail messages that were stored with a third-party communications service provider; they are authorized to obtain such information through executing a search warrant instead of an order for a wiretap search.

Prior to the USA PATRIOT Act of 2001's enactment, federal law enforcement's counterterrorism investigations were inhibited by complex, burdensome wiretap orders. § 209 made it easier for them to conduct surveillance of a target because they are now able to apply for a normal search warrant that would allow them to quickly seize voice-mail messages containing potentially incriminating information on a terrorist suspect.

Sec. 210. Scope of Subpoenas for Records of Electronic Communications.

§ 210 amends 18 U.S.C. 2703(c)(2), which details specific pieces of personal information, related to a subscriber or customer of communication services, that the providers of such services are allowed to share with governmental entities. Prior to the USA PATRIOT Act of 2001's enactment, the information that was authorized to be disclosed to government entities was limited and only included the targeted individual's name, address, local and long-distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of subscriber. Since the USA PATRIOT Act of 2001 was signed into law, providers of electronic communication or remote computing services are authorized to disclose the following identifying information unto a governmental entity: name, address, local and long distance telephone connection records or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service (including any credit card or bank account number) of a provider (Pub. L. 107-56, 2001). This provision is simply broadening the kinds of information and records which may be subpoenaed from communications providers for investigative purposes.

Sec. 211. Clarification of Scope.

§ 211 under Title II: Enhanced Surveillance Procedures amends § 631 of the Communications Act of 1934. More specifically, § 211 in the USA PATRIOT Act of 2001 amends § 631 "Protection of Subscriber Privacy" under the Communications Act by inserting a provision in § 631(c)(2) which, in other words, states that a cable operator is authorized to disclose personally identifiable information concerning a cable subscriber, pursuant to a court order, to a government entity as long as the disclosure does *not* include records which would indicate the "cable subscriber selection of video programming from a cable operator" (Pub. L. 117-338, 1934; Pub. L. 107-56, 2001). Federal law enforcement agencies and investigators are considered government entities, so this applies to them. In other words, this section facilitates information sharing between government entities and cable operators[14] by authorizing the operators to provide those entities with a cable subscriber's records and "personally identifiable information." The purpose of § 211 is to prevent a terrorist from escaping or "exempting" themselves from a lawful criminal investigation by means of choosing a cable company as their communication provider.[15] Prior to the USA PATRIOT Act of 2001's enactment, it was harder for cable subscribers to disclose personally identifiable information unto federal law enforcement agencies and/or investigators.

Sec. 212. Emergency Disclosures of Electronic Communications to Protect Life and Limb.

[14] 47 U.S.C. § 522(5)
[15] DOJ. (2004). Dispelling the Myths—The USA PATRIOT Act of 2001: MYTH VS. REALITY. Section 211. Clarification of Scope. *Department of Justice.*

§ 212 under Title II amends § 2702 and § 2703 of Title 18 to United States Code to authorize communications and computer-service providers to disclose records and communications in life-threatening emergencies (DOJ, 2023). The disclosure may be made to governmental entities such as federal law enforcement agencies, officers, and investigators. § 212 amends 18 U.S.C. § 2702 by inserting a statement which details the exceptions for the disclosure of customer records by communications and computer-service providers; the statement allows such providers to divulge records and information relating to a customer to a government entity "…if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information" (Pub. L. 107-56, 2001). § 212 amends 18 U.S.C. § 2703 by inserting a statement that describes how a governmental entity can require a provider, of either an electronic communication service or remote computing service, to disclose records and information pertaining to a subscriber or customer of such services (LII, 2023). In other words, under exigent circumstances, a provider of remote computing service or electronic communication service to the public may disclose to a federal law enforcement agency records or other personally identifiable information pertaining to a subscriber to or customer of such service(s) for investigatory purposes.

Sec. 213. Authority for Delaying Notice of the Execution of a Warrant.

§ 213 amends 18 U.S.C. § 3013a "Additional grounds for issuing warrant" by inserting a statement which explains that the immediate notification of the execution of a warrant or court order to search and seize property and/or materials that would contain evidence of a criminal offense in violation of the laws of the United States may be delayed in certain circumstances. Such circumstances that would permit such a delay are the following conditions:

(1) if the court has reasonable cause to believe that the immediate notification of the warrant being executed would cause an adverse result; or

(2) if the warrant prohibits the seizure of any tangible property, any wire or electronic communications, or any stored wire or electronic communications; or

(3) if the warrant, after its execution, provides for the giving of such notice within a reasonable period of time—the court may extend this period for 'good cause shown.' (Pub. L. 107-56, 2001).

Prior to the enactment of the USA PATRIOT Act of 2001, federal law enforcement had to immediately notify a suspect if they were executing a search warrant against them.

Sec. 214. Pen Register and Trap and Trace Authority Under FISA.

§ 214 amends § 402 and § 403 of FISA (50 U.S.C. 1842; 50 U.S.C. 1843). The amendments made by the USA PATRIOT Act of 2001 to the Foreign Intelligence Surveillance Act authorized FISA pen register and trap and trace orders for the purposes of obtaining foreign intelligence information and protecting against international terrorism or clandestine intelligence activities. Pertaining to the authorities established under § 214, the safeguard amendment made to § 402 requires the applicant(s) of the order to provide a certification, that is subject to approval by the Foreign Intelligence Surveillance Court (FISC), which ensures that the information that is likely to be obtained is truly foreign intelligence information that does not concern a U.S. person or is relevant to the continuing investigation being conducted for the purposes previously mentioned in this paragraph; it is required that such investigation is not to be conducted solely on the basis of the actions/activities protected and enshrined in the 1st Amendment to the United States Constitution. In addition, § 214 amends § 402 under FISA to expand the details in which the ex-

parte order, that approves the installation of a pen register or trap and trace device, must specify. The USA PATRIOT Act of 2001 (Pub. L. 107-56, 2001) lists that such specifications include the following details, if known, of the target of the investigation:

(i) the identity of the person;

(ii) "the identity…of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;"

(iii) the details of the communications to which this order applies, including the number or other identifier, and the location of the telephone line or other facility to which the pen register or trap and trace device is supposed to be attached or applied and, in the instance of a trap and trace device, the geographic limits of the trap and trace order.

§ 214 amends § 403 under FISA to clarify that an Attorney General may make a determination that an emergency requires the installation and use of a pen register or trap and trace device to obtain foreign intelligence information, that does not concern a U.S. person, or information to protect against international terrorism or clandestine intelligence activities. The safeguard, like that in § 402, is that such investigations are not to be conducted solely on the basis of the activities protected in the 1st Amendment to the U.S. Constitution.

Sec. 215. Access to Records and Other Items Under the Foreign Intelligence Surveillance Act.

§ 215 amends the Foreign Intelligence Surveillance Act of 1978 by removing § 501–503 and replacing it with § 501 "Access to Certain Business Records Under the Foreign Intelligence Surveillance Act" and § 502 "Congressional Oversight" (Pub. L. 107-55, 2001). § 215 provides an authorization for the federal government to access and obtain business, library, and computer

records gathered in terrorism investigations through hearings of the FISC (Foreign Intelligence Surveillance Court) (Deflem & McDonough, 2015: Denniston, 2003). The Select Committee on Intelligence (2005) clarified that § 215 in Title II of the USA PATRIOT Act of 2001 "…broadened the scope of records that could be sought to 'any tangible things,'…it allowed the FBI to make an application 'for an investigation' to protect against international terrorism or clandestine intelligence activities." It should be noted that such investigations of a U.S. person cannot be conducted solely on the basis of activities protected by the 1st Amendment to the United States Constitution. On the other hand, § 215 allows the FISC to issue an ex-parte order requiring the production of the tangible things previously mentioned for the purpose of protecting against international terrorism and clandestine intelligence activities; an ex-parte order may be entered to approve for the release of business records for foreign intelligence and international terrorism investigations (DOJ, 2004; Pub. L. 107-56, 2001).

Section 215 of the USA PATRIOT Act of 2001 establishes congressional oversight. On a semiannual basis, the Attorney General must "fully inform" the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate on how § 215 was used; the Attorney General must provide a report detailing all requests for the production of tangible things, including the orders that were either granted, modified, or denied (DOJ, 2004; Pub. L. 107-56, 2001).

Sec. 216. Modification of Authorities Relating to Use of Pen Registers and Trap and Trace Devices.

§ 216 amends sections 3121(c), 3123(a), 3123(b)(1), 3123(d)(2), 3127(2), 3127(3), 3127(4), 3127(1), 3124(d), and 3124(b) of title 18, United States Code, to increase and enhance

federal law enforcement agencies' investigative abilities by apply ex-parte orders that would allow them to install their own pen register or trap and trace devices on a "packet-switched data network of a provider of electronic communication service to the public" in order to electronically record any and all information collected from such devices. Such information is critical to investigators because it includes valuable data including the outgoing phone numbers dialed from a particular telephone (collected from a pen register), the incoming phone numbers dialed to a particular telephone (collected from a trap and trace device), and the utilization of such devices to record *all* computer routing, addressing, and signaling information (EPIC, 2023). Under the USA PATRIOT Act of 2001, § 216 allows courts to issue pen register or trap and trace device orders that are applied to Internet communications, in addition to that are valid and applicable across the country (DOJ, 2004). Section 216 also clarifies terms including "court of competent jurisdiction," "pen register," "trap and trace device," "conforming amendment," and "technical amendment."

Sec. 217. Interception of Computer Trespasser Communications.

§ 217 of the USA PATRIOT Act of 2001 amends the Wiretap Act of 1968, specifically sections 2510 and 2511(2) in Chapter 119 of title 18, United States Code, to "…[allow] victims of computer-hacking crimes to request law-enforcement assistance in monitoring trespassers on their computers" (DOJ, 2004). § 217 allows law enforcement to intercept the wire or electronic communications of a computer trespasser* that was transmitted to, through, or from a protected computer*. In other words, this section enhances terrorism investigations and surveillance of terrorists by allowing federal law enforcement to obtain communications related to computer

trespassers from the owner/operator of the protected computer that was hacked by said trespasser.

Prior to the enactment of the USA PATRIOT Act of 2001, federal law enforcement was not permitted to intercept wire or electronic communications of a computer trespasser. Now, an owner/operator of a protected computer can request assistance from federal law enforcement entities.

Sec. 218. Foreign Intelligence Information.

§ 218 of the USA PATRIOT Act of 2001 amends §104(a)(7)(B) and §303(a)(7)(B) of the Foreign Intelligence Surveillance Act by replacing the phrase "the purpose" with "a significant purpose." Originally, §104(a)(7)(B) required an entity to certify that "the purpose" of conducting electronic surveillance was to obtain foreign intelligence information (Pub. L. 95-511, 2008; Select Committee on Intelligence, 2005. § 218 of the USA PATRIOT Act of 2001 changed this wording to expand the ability of a federal officer to apply for an order that would approve their usage of FISA surveillance for not "the purpose," but "a significant purpose" of collecting foreign intelligence information (Pub. L. 107-56 2001). In other words, federal law enforcement officers and investigators seeking the acquisition of court orders for warrants under the USA PATRIOT Act of 2001 no longer needed to prove that obtaining foreign intelligence information was the one and only purpose behind their surveillance efforts.

Sec. 219. Single-Jurisdiction Search Warrants for Terrorism.
Sec. 220. Nationwide Service of Search Warrants for Electronic Evidence.

Sections 219 and 220 are closely related in that they make amendments to previous legislation in order to expand the geographic scope of search warrants for terrorism and electronic evidence. § 219 amends rule 41(a) of the Federal Rules of Criminal Procedure, while § 220 amends sections 2703, 2703(d), and 2711 in Chapter 121 of title 18, United States Code. Section 219 maximized the amount of law enforcement officers and personnel that are available to assist in terrorism-related investigations. Section 220 under the USA PATRIOT Act of 2001 allows courts with jurisdiction over the offense under investigation to obtain search warrants for communications that are being stored by providers in any location across the country (DOJ, 2004).

Prior to the enactment of the USA PATRIOT Act of 2001, courts were only able to approve search warrants in their jurisdiction. § 219 changed this to allow search warrants for terrorism to be issued for a person and/or property outside of a court's jurisdiction. § 220 changed this by allowing a nationwide search warrant for electronic evidence to be issued as long as the warrant is ordered by a court with jurisdiction over the offense.

Amendments to Existing Legislation by the USA PATRIOT Act of 2001

Sections that Amend the Foreign Intelligence Surveillance Act of 1978	§ 206, 207, 208, 214, 215, 218

Sections that Amend the Wiretap Act of 1968	§ 203, 209, 217
Sections that Amend the Communications Act of 1934	§ 211

Part II. Applying the Related Sections to Research Question, Theoretical Propositions, and Rival Explanations

Research Question: How has the USA PATRIOT Act of 2001 impacted the way that federal law enforcement conducts the surveillance of terrorist activity in the United States?

Initial Theoretical Proposition and Explanation: The enactment of the USA PATRIOT Act of 2001 has made it easier for federal law enforcement agencies, officers, and investigators to conduct surveillance in the United States and target and eliminate terrorist threats by broadening and expanding the authorizations granted to them by prior legislative acts that allowed them to use electronic surveillance technology to monitor and track terrorists and their crimes. Title II: Enhanced Surveillance Procedures of the USA PATRIOT Act of 2001 strengthens United States counterterrorism strategies through its amending of legislation, such as the Foreign Intelligence Surveillance Act of 1978, the Wiretap Act of 1968, and the Communications Act of 1934, all of, which established broad authorities for federal law enforcement's use of surveillance tools in their counterterrorism investigations and created guidelines for the interception of communications for law enforcement investigatory purposes. The theory being developed in this

thesis explains that the USA PATRIOT Act of 2001 was a groundbreaking piece of counterterrorism legislation which heavily affected federal law enforcement's surveillance of terrorist acts in or against the United States by authorizing them to use enhanced surveillance technology and procedures in their investigations.

- *Rival Explanation:* At the very core of Title II: Enhanced Surveillance Procedure lies a contradictory approach to U.S. counterterrorism strategies. The expansion of federal law enforcement's authorities regarding the monitoring, interception, and sharing of wire, oral, and electronic communications relating to terrorism and computer fraud and abuse offenses, and the increase in sophisticated surveillance procedures being utilized by federal law enforcement utilizes has bred a culture of fear which has negatively impacted the general public's confidence in the U.S. government's ability to mitigate and prevent terrorist activity, thus impacting the effectiveness of such strategies and therefore reducing the likelihood that federal law enforcement is able to destroy the threats of terrorism. Title II's impact on federal law enforcement's authorities related to their now expanded use of surveillance procedures and sophisticated surveillance technology for the purpose of monitoring terrorist activity has produced substantial backlash in the public eye due to a widely held perception of the invasion of privacy and, ultimately, a violation of the civil liberties bestowed upon every American citizen. Although Title II: Enhanced Surveillance Procedures under the USA PATRIOT Act of 2001 enhanced federal law enforcement's counterterrorism strategies and investigations, it cultivated a culture of government resistance by producing deeply rooted fears that the government is violating the First, Fourth, and Fifth Amendments to the United States Constitution by

illegally monitoring and obtaining personal information and communications from innocent Americans.[16]

Final Theoretical Proposition and Explanation: Title II: Enhanced Surveillance Procedures of the USA PATRIOT Act of 2001 impacted federal law enforcement's surveillance of terrorism in the United States by making amendments to previous legislation which widened the scope of authority they possess surrounding the interception, monitoring, sharing, and utilization of the information gathered from, as well as the technology utilized in, the following: wire, oral, and electronic communications relating to terrorism and computer fraud and abuse offenses[17], criminal investigations and grand jury matters[18], roving surveillance including wiretaps and warrants[19], foreign intelligence investigations[20], pen registers and trap and trace devices/orders for electronic communications[21], computer trespasser communications[22], any tangible things, such as business, library, and computer records[23], voice-mail messages[24] and FISA surveillance and search warrants for property, persons, or electronic evidence[25]. Seventeen provisions under Title II: Enhanced Surveillance Procedures explicitly detail the improvements made to the surveillance procedures implemented by federal law enforcement agencies and investigators; these provisions facilitated the tools utilized by such entities in their execution of U.S. counterterrorism strategies aimed towards preventing, mitigating, and eliminating acts of

[16] Deflem & McDonough. (2015); DOJ. (2004).
[17] § 201, 202. *Pub. L. 107-56 (2001)*
[18] § 203. *Pub. L. 107-56 (2001)*
[19] § 206. *Pub. L. 107-56 (2001)*
[20] § 218. *Pub. L. 107-56 (2001)*
[21] § 214, 216. *Pub. L. 107-56 (2001)*
[22] § 217. *Pub. L. 107-56 (2001)*
[23] § 215. *Pub. L. 107-56 (2001)*
[24] § 209. *Pub. L. 107-56 (2001)*
[25] § 207, 219, 220. *Pub. L. 107-5 (2001)*

terrorism that continue to threaten the state of national security in the United State. Section 201 amended prior legislation to allow for FISA search and surveillance orders to be applied to terrorism investigations conducted by federal law enforcement. Sections 201 and 202 gave federal law enforcement the authority to intercept wire, oral, and electronic communications in investigations of terrorism and computer fraud and abuse offenses that target a wider range of crimes, such as: using chemical weapons & WMDs; violating criminal penalties under 18 USC 2332; committing acts of terror in foreign/international countries; providing resources/material & financial support to foreign organizations and operations; and engaging in financial transactions with foreign governments that support international terrorism. Section 203 enabled federal law enforcement agencies, officers, and investigators to have matters involving foreign intelligence or counterintelligence or foreign intelligence information disclosed to them. Section 206 authorized federal law enforcement to implement FISA surveillance methods such as "roving" warrants if they have cause to believe that the actions of the target of their investigation may thwart/inhibit (make it more difficult to conduct) the surveillance of their actions. Section 207 amended the Foreign Intelligence Surveillance Act of 1978 to extend the maximum duration of FISA search and surveillance orders applying for electronic surveillance and physical searches targeting both United States and non-United States persons. Section 209 authorized federal law enforcement to use search warrants instead of wiretaps to obtain or "seize" voice-mail messages from a third-party communications service provider for investigative purposes. Section 210 expanded the scope of subpoenas for electronic records by authorizing federal law enforcement agencies to require an internet service provider to disclose information about their customers including their name, address, telephone connection records/records of session times and durations, length and type of service used, telephone number/instrument number/subscriber

number or identity/temporarily assigned network addresses, and credit card and bank account numbers; this provided federal law enforcement with the enhanced ability to conduct more thorough surveillance of a target. Section 211 amended the Communications Act of 1934 to authorize cable operators to provide Federal law enforcement with a cable subscriber's records and "personally identifiable information." Section 212 stated that, under exigent circumstances, a provider of remote computing service or electronic communication service to the public may disclose to a Federal law enforcement agency records or other personally identifiable information pertaining to a subscriber to or customer of such service(s) for investigatory purposes. Section 213 authorized federal law enforcement to delay notifying a suspect that they have executed a search warrant targeting their persons or property, thus allowing them to extend the period of surveillance. It authorized federal law enforcement 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" without providing immediate notification. Section 214 amended the Foreign Intelligence Surveillance Act of 1978 to authorize federal law enforcement to use pen register and trap and trace surveillance to target both U.S. and non-U.S. persons for investigations aimed towards obtaining information relating to foreign intelligence or for investigations aimed towards protecting against international terrorism and/or clandestine intelligence activities. Section 215 amended the Foreign Intelligence Surveillance Act of 1978 to authorize federal law enforcement to apply for an order allowing them to access and obtain "tangible things" like books, records, papers, and documents for their counterterrorism investigations. Section 216 authorized federal law enforcement to apply ex-parte orders that would allow them to install their own pen register or trap and trace devices on a "packet-switched data network of a provider of electronic communication service to the public" in order to electronically record any and all information

collected from such devices for the purpose of collecting critical information pertaining to a criminal or terror-based investigation. Section 217 authorized federal law enforcement to monitor, surveil, and intercept the communications of computer hackers. Section 218 amended the Foreign Intelligence Surveillance Act of 1978 to authorize federal law enforcement to conduct surveillance in a terrorism investigation as long as the gathering of foreign intelligence information is the *significant* purpose—it no longer needs to be *the* purpose of the investigation. Section 219 authorized federal law enforcement to execute a search warrant for property or for a person within or outside the district of application for the purpose of investigating domestic or international terrorism. Section 220 authorized federal law enforcement to execute a search warrant for electronic evidence, thus allowing them to obtain a suspect's communications from a provider in any location across the country. Prior to the USA PATRIOT Act of 2001, federal law enforcement and other government entities were not authorized to use electronic surveillance procedures for a wide array of terror-based crimes. The provisions under Title II widened the scope of crimes that could be surveilled by federal law enforcement. Logically, the depth of their terrorism investigations has increased substantially, thus allowing them to be better equipped to target and eliminate terrorist threats.

- *Rival Explanation:* The safeguard procedures instilled in the seventeen provisions under Title II of the USA PATRIOT Act of 2001, relating to federal law enforcement's surveillance of terrorist activity in the United States, are only effective if the procedures are properly documented and carried out; this places an exorbitant amount of faith in the entities involved in disclosing the reports that hold federal law enforcement agencies and investigators accountable for the execution of FISA surveillance or search orders that

> aims to obtain information whose contents include foreign intelligence or counterintelligence, or foreign intelligence information.

At the very heart of sections 201 and 202 lies the integral role that federal law enforcement plays in counterterrorism. They are directly involved in the active interception of wire, oral, and electronic communications relating to terrorism. Specifically, federal law enforcement agencies, officers, and investigators are authorized to intercept such communications when that interception may provide or has provided evidence that a person(s) has committed criminal violations or penalties relating to chemical-weapons offenses, the use of WMDs, acts of terrorism abroad, terrorism financing, providing material support to terrorists and/or providing material support or resources to foreign terrorist organizations (Pub. L. 107-56, 2001; DOJ, 2023). Section 202 impacted investigative methods authorized by FISA when it amended the FISA definition of "foreign intelligence information" to be inclusive and applicable to critical information relating to the United States's protection against threats to national security (Roberts, 2005). Roberts (2005) explains that § 202 had a profound impact on federal law enforcement's surveillance of terrorist activity in the United States because it "…fully integrated intelligence and law enforcement components" and subsequently ensured that the President of the United States would be able to "…use all lawful means…to prevent and neutralize threats to the national security" (Roberts, 2005).

The Department of Justice (2004) dispelled a myth surrounding § 203 of the USA PATRIOT Act of 2001. The American Civil Liberties Union (2001) was quoted as saying that there are no 'safeguards' to ensure that this sharing of information is appropriate in the sense that it is not violating civil liberties of innocent American citizens (DOJ, 2004; ACLU, 2001). The

notion that there are no safeguards preventing federal law enforcement from abusing their authority to share criminal investigative information under this section is unfounded and untrue. While § 203 authorizes the sharing of grand jury and wiretap information, regarding foreign intelligence, with federal law enforcement, intelligence, protective, immigration, national defense, and national security personnel, there are numerous safety provisions underlined throughout this section that would prevent misuse of the information being shared. For starters, § 203(a)(1)(iii) amends Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure (FRCP) to provide a safeguard that would require an attorney for the United States government to file under seal, a notice that would explicitly present and state all facts relative to the information that was disclosed as well as the entities to which such disclosure of information was made; this provision also emphasizes that any federal law enforcement agency, official, or other government entity to which information was disclosed must use this information "…only as necessary in the conduct of that person's official duties subject to an limitations on the unauthorized disclosure of such information" (Pub. L. 107-56, 2001). In addition, § 203(d)(1) states, "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" (Pub. L. 107-56). In other words, any individual receiving information that is pursuant to this provision can only use such information on the basis of pure necessity. In addition to this, § 203(c) lists an additional safeguard which requires the Attorney General to establish and specifically outline procedures regarding the disclosure of information pursuant to § 2517(6) and Rule 6(e)(3)(C)(i)(V) of the Federal Rules of Criminal Procedure; § 2517(6) underlines the authorization bestowed upon "any investigative or law enforcement officer, or attorney for the Government" to engage in the disclosure and use of intercepted wire, oral, or

electronic communications (18 U.S.C. § 2517(6). § 203 impacted the way that law enforcement conducts the surveillance, with the intention of targeting, mitigating, and eliminating acts of terrorism, by facilitating a more coordinated and integrated counterterrorism and antiterrorism campaign (DOJ, 2004). § 203 ultimately allows federal law enforcement to gain deeper awareness and understanding with regard to grand jury and wiretap information that involved foreign intelligence. § 203 enables federal law enforcement agencies, officers, and investigators to be more involved in matters relating to foreign intelligence gathering and criminal investigative information, especially that which is pertinent to U.S. counterterrorism strategies. § 203 has reduced the statutory and cultural barriers to information sharing which ultimately hindered national security investigations pre-9/11 (Select Committee on Intelligence, 2005). The overall impact that § 203 has had on the conduct of federal law enforcement related to counterterrorism efforts is profound in the sense that this provision has made it easier to detect and disrupt terrorist plots. Subsequently, federal law enforcement's surveillance procedures used to monitor terrorism in the United States were enhanced through the enactment of this provision—the sharing of information pursuant to § 203 facilitates more thorough and effective counterterrorism-related investigations. § 203 aligns with my theoretical proposition which explains how Title II: Enhanced Surveillance Procedures under the USA PATRIOT Act of 2001 was effective in strengthening and solidifying U.S. counterterrorism strategies because this provision directly affects the surveillance procedures implemented by federal law enforcement agencies and investigators. This notion is supported by statements made in the Select Committee on Intelligence's report on provisions under the USA PATRIOT Act of 2001: "FBI agents in several field offices provided…specific examples of cases in which they were able to use the USA PATRIOT Act of 2001 information access provisions to neutralize targets in non-traditional

ways" (Select Committee on Intelligence, 2005). § 203 has impacted federal law enforcement's surveillance of terrorist activity by allowing for the disclosure of vital information which is used in the dismantling of terror cells. Gonzales and Mueller (2005) explain how § 203 is frequently relied upon by federal law enforcement agencies such as the FBI because the provision facilitates information sharing with regard to criminal investigations between them and the National Counterterrorism Center (NCC) in order to successfully detect and destroy terrorist threats.

Section 206 is, perhaps, one of the most impactful provisions underlined in Title II: Enhanced Surveillance Procedures. Despite it being one of the shorter sections in this portion of the USA PATRIOT Act of 2001, § 206 heavily impacted federal law enforcement's surveillance procedures utilized in their counterterrorism strategies and investigations by establishing the authority for them to use "roving wiretaps" in counterterrorism investigation. According to the Select Committee on Intelligences' report, "Roving wiretaps permit electronic surveillance of people who may be taking steps, such as switching cell phones or using multiple pay phones or computer terminals, to evade electronic surveillance at a particular location" (Roberts, 2005). The utilization of such wiretaps existed prior to the USA PATRIOT Act of 2001's enactment; however, the wiretaps were only being applied to ordinary criminal investigations. Section 206 authorized the application of FISA wiretaps for terrorism-related investigations, thus impacting the execution of surveillance of terrorist activity by allowing federal law enforcement to take advantage of roving wiretaps for national security investigations (DOJ, 2004). There is controversy surrounding this particular section of the USA PATRIOT Act of 2001 that is exacerbated by the myth that the expansion of federal law enforcement's power and authority under § 206, with regard to roving wiretaps, was done in "secret" and without consideration for protecting the privacy of innocent Americans (DOJ, 2004). The Department of Justice negates

this myth by their emphasis on the vital role that the Foreign Intelligence Surveillance Court (FISC) plays in the approval of the roving warrants and wiretaps that are requested by federal law enforcement in their investigations.

Section 207 impacts federal law enforcement's surveillance of terrorist activity by extending the maximum duration of electronic surveillance and physical searches pursuant to FISA and making the time periods equivalent for both (Select Committee on Intelligence, 2005). This provision has streamlined the processing of FISA applications by federal law enforcement, specifically the Federal Bureau of Investigation, making for more effective investigations by allowing for combined electronic surveillance and physical search applications (Select Committee on Intelligence, 2005). The Select Committee on Intelligence (2005) explained how § 207 was instrumental in enhancing federal law enforcement's counterterrorism strategies by allowing the Federal Bureau of Investigation and the Department of Justice's Office of Intelligence Policy and Review (OIPR) to conserve the limited resources they use to process FISA surveillance or search applications by making the time periods equivalent for both types of orders. Essentially, § 207 impacts federal law enforcement by allowing them to conduct surveillance on their target for a longer period of time.

Section 209 impacts the surveillance of terrorist activity by federal law enforcement because they are now able to obtain key evidence from voice-mail messages either left for or left by terrorists, both foreign (international) and domestic in nature. Burdensome wiretap orders put restrictions on investigations by federal law enforcement that made it harder for terrorist activity to be monitored. Now, under § 209, the processes of monitoring, surveillance, and collecting critical information related to a suspect is more streamlined for such governmental entities; it is

now easier for them to access vital information that can be collected from voice-mail messages in their pursuit of a terrorist.

Section 210 impacted the way that governmental entities, specifically federal law enforcement, conducts surveillance of terrorist activity by expanding the type of personal information and relevant identifying records that can be utilized in investigation The DOJ (2023) emphasizes that § 210 was an important update to the law because it facilitated more thorough and effective surveillance procedures by providing the full range of information pertaining to a suspect. The DOJ (2023) highlights this notion by explaining that the newfound authorities established under § 210 allows law enforcement to monitor and quickly trace suspects by using information related to the suspect/customer's means of payment such as "any credit card or bank account number" (DOJ, 2023; Pub. L. 107-56, 2001). Section 210 of the USA PATRIOT Act of 2001 expanded the subpoenas for electronic information which affected federal law enforcement agencies surveillance of terrorist activity by "…requir[ing] internet service providers to disclose information about their customers…" (EPIC, 2023). The DOJ (2004) explains that this expansion under § 210 allows for federal law enforcement to quickly trace the target(s) under the scope of their investigation by providing these entities with invaluable and indispensable information that is imperative for the successful tracking of a suspect.

Section 211 under Title II applies directly to the theoretical proposition driving this thesis, which explains that such provisions under the USA PATRIOT Act of 2001 have strengthened and solidified U.S. counterterrorism strategies by expanding the scope and depth of federal law enforcement's investigations into terrorist activity. § 211 is saying that government entities, including federal law enforcement, are authorized to obtain personally identifiable information concerning an individual being targeted by their investigation. Thus, their processes

of monitoring and surveillance of terrorist activity are enhanced because federal law enforcement is now able to access even more data regarding someone under investigation whom they believe to be engaging in terrorist activity, as defined in Title IV of the USA PATRIOT Act of 2001.

Section 212 is a critical provision under the USA PATRIOT Act of 2001 that can be applied to surveillance of terrorist activity by federal law enforcement agencies, officers, and investigators. The disclosure of communications authorized by this provision may be made to government entities, such as federal law enforcement, to aid in investigations, specifically those involving acts of terrorism. This provision enhances federal law enforcement's surveillance of terrorist activity because, under § 212, they are now able to receive information that would have otherwise been unauthorized/prohibited from receiving. The Department of Justice (2023) emphasizes the importance of this provision in Title II: Enhanced Surveillance Procedures in their example of an Internet service provider realizing that a customer was going to commit a terrorist attack. Under § 212, the Internet service provider would be allowed to notify law enforcement and disclose information, data, and reports pertinent to the customer to them with the intention of preventing and/or mitigating such an attack. In addition, § 212 prevents the communications provider from being subject to civil lawsuits (DOJ, 2023). § 212 impacts federal law enforcement's surveillance of terrorist activity by facilitating information sharing between this entity and communications service providers; now, federal law enforcement is better equipped to combat terrorism since they are able to conduct more thorough investigations by monitoring activity and accessing information and reports that, prior to the enactment of the USA PATRIOT Act of 2001 and § 212, was not allowed to be accessed/disclosed to them without the fear of the service providers being subject to lawsuits about violations of civil liberties. § 212 enhances law enforcement's surveillance of terrorist activity by authorizing communications

providers to disclose key information about a suspect that would streamline counterterrorism investigations.

Section 213 affected the way that law enforcement handles investigations, specifically those involving acts of terrorism or acts in the preparation thereof. Section 213 pertains to federal law enforcement's investigations of serious crimes, especially those which involve acts of domestic and/or international terrorism (DOJ, 2004). The amendments made to 18 U.S.C. § 3103a established that, under a specific set of circumstances, law enforcement is authorized to delay notice of the execution of a warrant or court order to allow for the agents to investigate a suspect without that individual being aware of the active investigation surrounding themself. This provision under the USA PATRIOT Act of 2001 enhanced the monitoring and surveillance of targets being suspected of engaging in terrorist activity by allowing federal law enforcement agencies and officers to conduct searches pursuant to the warrant being executed without compromising their investigation. The myth perpetuated by the ACLU (2003) that this section under the USA PATRIOT Act of 2001 was essentially violating the civil liberties of innocent Americans because the provision expanded the ability for the government to conduct searches of private property without giving any notice to the owner of such property was a false and unfounded claim; the Department of Justice negates this by arguing that there are only certain narrow circumstances which necessitate the delayed notice of a search warrant execution (DOJ, 2004). The court must find reasonable cause that delaying the notification of a search warrant execution would have an adverse effect before they would approve the application for an order to install and use a pen register or trap and trace device. § 213 is critical for federal law enforcement's surveillance of terrorism because the provision allows them to monitor terrorist activity and collect information from their investigation for a longer period of time before they

are required to notify their target that they have executed a search warrant permitting such surveillance. Relating this to my theoretical proposition, § 213 is another provision under Title II: Enhanced Surveillance Procedures in the USA PATRIOT Act of 2001 which strengthened U.S. counterterrorism strategies implemented by federal law enforcement agencies and officers by improving the investigative procedures they employ in order to effectively "…locate their terrorists or criminal associates, identify and disrupt their plans, [and] initiate their arrests" (DOJ, 2004).

Section 214 was an important provision under the USA PATRIOT Act of 2001 because it "…made the standard contained in the FISA for obtaining an order for a pen register or trap and trace device consistent with the standard for obtaining an order for a criminal pen register or trap and trace device" (Roberts, 2005). § 214 authorized Federal law enforcement to use pen register and trap and trace surveillance to target both U.S. and non-U.S. persons for investigations aimed towards obtaining information relating to foreign intelligence or for investigations aimed towards protecting against international terrorism and/or clandestine intelligence activities. Section 214 impacted surveillance of terrorism through its design which broke down the "wall" or the obstacle that prevented the sharing and dissemination of foreign intelligence information to federal law enforcement agencies and investigators.

Section 215 of the USA PATRIOT Act of 2001 impacted federal law enforcement's surveillance of terrorist activity by broadening the range of tangible things which may be produced by their investigation aimed towards protecting against international terrorism and/or clandestine intelligence activities. It streamlined counterterrorism strategies by authorizing the FBI to obtain books, records, papers, documents, and other items that are determined to be evidence in such an investigation. Under this provision, the Federal Bureau of Investigation,

which is a governmental entity, is able to gather more extensive information pertaining to a subject under their investigation by applying for an order requiring such things to be released for the purpose of furthering that investigation. Federal law enforcement is now able to conduct more thorough surveillance procedures because they are able to access and monitor tangible records pertaining to the target which may contain critical information that could potentially reveal acts of international terrorism or clandestine intelligence activities, or actions in the preparation thereof. According to a government article which dispels myths surrounding the USA PATRIOT Act of 2001, § 215 "…expanded the types of entities that can be compelled to disclose information"; prior to the USA PATRIOT Act of 2001, the scope of records which federal law enforcement agencies, specifically the Federal Bureau of Investigation, could obtain for such investigations was extremely limited. In contrast, a common criticism of this section of the USA PATRIOT Act of 2001 is that its narrow scope does not apply to investigations into domestic terrorism-related incidents; in investigations of United States persons, § 215 can only be applied if the business records obtained from this person are used to protect against international terrorism or clandestine intelligence activities (DOJ, 2004).

Section 216 applies to federal law enforcement's surveillance of terrorist activity by amending the statutes involved with their use of pen registers and trap and trace devices in terrorism-related investigations; Section 216 changed such statutes to apply it to Internet communications (DOJ, 2004). This was a pivotal provision under the USA PATRIOT Act of 2001 that updated the laws to reflect the newer technology utilized by terrorists and, ultimately, enhance federal law enforcement's surveillance capabilities. The Department of Justice (2004) explained that § 216 allowed such entities to gather more information for their investigation by using pen register or trap and trace device orders to not only track which numbers that a

particular phone dials, but also gather the same type of information about communications transmitted through the Internet. Section 216 impacted law enforcement's surveillance of terrorist activity by limiting federal law enforcement agencies to install and use a pen register and/or trap and trace device by restricting the device from collecting the content of any wire or electronic communication gathered from said communications. The DOJ (2004) explains that § 216 is used in obtaining critical information that can help federal law enforcement identify key suspects in terrorism cases; law enforcement can utilize a pen register device's collection of routing and addressing information to track these suspects in addition to merely identifying them. The safeguard enshrined within this provision ensures that a federal law enforcement agency must report to the FISC anytime it executes a pen register or trap and trace device order. Through the enactment of section 216 under the USA PATRIOT Act of 2001, federal law enforcement can monitor, and record information related to computer routing, addressing, and signaling (EPIC, 2023).

Section 217 impacted federal law enforcement's surveillance of terrorism by allowing them to monitor and intercept the communications of a computer trespasser if they are requested to do so by the operator of the protected computer that was unlawfully accessed by the trespasser. Law enforcement, under § 217, can provide significant aid in investigations where terrorists illegally trespassed on a protected computer. Prior to the USA PATRIOT Act of 2001, law enforcement was not allowed to intercept computer trespasser information from a computer service provider because the law prohibited the provider from sharing such information. § 217 is an invaluable provision for federal law enforcement because it makes the law "technology-neutral" in that terrorists who are cyber-trespassers are on the same level as terrorists who are "physical intruders" (Martinez, 2005). The safeguard in place within this provision ensures that

federal law enforcement can only monitor and intercept the communications of a trespasser if they are requested and authorized to do so by the owner or operator of the protected computer (Pub. L. 107-56 (2001)). Section 217 facilitates federal law enforcement's surveillance of terrorist activity by expanding the scope of crimes of terrorism they are allowed to monitor. The Department of Justice (2004) emphasizes this facilitation by expressing that § 217 of the USA PATRIOT Act of 2001 enhances the gathering of evidence regarding crimes of computer trespassing, especially in terrorism investigations or cases where national security is being threatened. § 217 is an imperative provision which involves federal law enforcement in a wider range of acts of terrorism, specifically computer hacking crimes where a provider has detected that a terrorist has unlawfully breached a protected computer.

Despite section 218 being one of the shorter provisions under the Act, it is perhaps one of the most influential regarding the impact of the USA PATRIOT Act of 2001 on the implementation of newly enhanced surveillance procedures for federal law enforcement to fight the U.S.'s continuing battle against terrorism. Unfortunately, it is one of the more controversial parts of the USA PATRIOT Act of 2001. One reason behind the debate surrounding § 218 explains that it does not define the scope behind "a significant purpose," thus leaving the interpretation of the term 'significant' up for debate. Whitehead (2002) argues that § 218 allows federal law enforcement to apply the "loose" standards under FISA to their investigations, which primarily target American citizens and residents, that are only partly focused on national security. Rackow (2002) mentions that this provision under the USA PATRIOT Act of 2001 will lead to federal law enforcement and intelligence officers applying for warrants to conduct electronic surveillance despite their primary purpose of the FISA investigation being a criminal investigation while their collection of foreign intelligence information is merely a secondary

purpose. In my opinion, § 218 was a necessary provision to enhance federal law enforcement's surveillance of terrorist activity; the Select Committee on Intelligence (2005) supports this notion by explaining that § 218 "Foreign Intelligence Information" permits federal law enforcement to conduct electronic surveillance and/or a physical search to collect information and evidence in order to protect "…national security by the criminal prosecution of any foreign intelligence crime the target may have committed or intends to commit." § 218 is a key section in the USA PATRIOT Act of 2001 which directly affected the surveillance of terrorism by federal law enforcement. Section 218 broke down a "wall" that stood between law enforcement and intelligence investigators; this "wall" was restricting critical information sharing necessary for effectively countering acts of terrorism or acts in preparation thereof (DOJ, 2004; Select Committee on Intelligence, 2005). Prior to the enactment of the USA PATRIOT Act of 2001, terrorism investigations were largely inhibited by this "wall" which only allowed federal law enforcement to seek a FISA order if the intention of collecting foreign intelligence was the *sole* purpose of the investigation; § 218 broke it down by eliminating the requirement for FISA surveillance or searches to be conducted under a certification that "the purpose" of this type of investigation was to obtain foreign intelligence information. Now, federal law enforcement is able to better target acts of terrorism even if they are only tangentially related to the gathering of foreign intelligence information. This is an important provision for federal law enforcement's surveillance of terrorist activity because it has had a tangible effect on United States's counterterrorism strategies; § 218 led to the successful facilitation of the disruption of terrorist plots, the apprehension of terrorists, and convictions in cases of terrorism (Gonzales & Mueller, 2005).

Sections 219 and 220 are provisions that are imperative for the success of counterterrorism investigations headed by federal law enforcement. The amendments made within those sections facilitated the authorization to execute a search warrant in a jurisdiction different than that in which the court who applied for the search warrant order resides. Prior to the enactment of the USA PATRIOT Act of 2001, many time-sensitive, terrorism-related investigations were delayed because the warrants that investigators requested were often for faraway jurisdictions (DOJ, 2004). Under these provisions, federal law enforcement is better equipped to conduct surveillance of terrorist activity because the search warrants are no longer limited to a single jurisdiction. Conclusively, § 219 and 220 under Title II of the USA PATRIOT Act of 2001 helped eliminate the burden of a time-sensitive investigation of terrorist networks which typically span across numerous jurisdictions; these provisions impact federal law enforcement by expanding their scope of surveillance to cover any judicial district in the United States (DOJ, 2004).

These seventeen sections under the USA PATRIOT Act of 2001 are all relevant to federal law enforcement's surveillance of terrorist activity. Pre-9/11 legislation like the Foreign Intelligence Surveillance Act of 1978 gave very broad authorities to law enforcement for surveillance of terrorist activity. The enactment of the USA PATRIOT Act of 2001 and solidification of surveillance by provisions in Title II: Enhanced Surveillance Procedures resulted in the ability for Federal law enforcement to conduct more thorough terrorism-related investigations by authorizing them to use a wider range of surveillance tools that would apply to more crimes of terror. One such example of this is highlighted in § 201 in Title II authorized Federal law enforcement to intercept wire, oral, and/or electronic communications if they believe that the interception would provide, or has provided, evidence of a terrorist unlawfully

developing, producing, acquiring, transferring, receiving, stockpiling, retaining, owning, possessing, using, or threatening to use any chemical weapon.[26] In the next Chapter, the significant findings of this case study analysis are summarized and tied to the theoretical propositions that were developed throughout this thesis. Chapter 5 also discusses the limitations I faced when conducting research, alternative decisions I would make if I redid this study, suggestions for future research and policy implications, and the benefits of this work.

Chapter 5 – Conclusion

Part I. Summary of Major Findings

The final theoretical proposition for this case study analysis is the following: Title II: Enhanced Surveillance Procedures of the USA PATRIOT Act of 2001 impacted federal law enforcement's surveillance of terrorism in the United States by making amendments to previous legislation which widened the scope of authority they possess surrounding the interception, monitoring, sharing, and use of the information gathered from, as well as the technology utilized in, the following: wire, oral, and electronic communications relating to terrorism and computer fraud and abuse offenses, criminal investigations, roving wiretaps and warrants, foreign intelligence investigations, pen registers and trap and trace devices/orders, computer trespasser communications, any tangible things, such as business, library, and computer records, voice-mail messages and FISA surveillance and search warrants for property, persons, or electronic evidence.

[26] § 201. *Pub. L. 107-56 (2001)*; 18 U.S.C. § 229(a)(1)

How exactly did the USA PATRIOT Act of 2001 strengthen U.S. counterterrorism strategies? This Act facilitated a more expansive and in-depth investigation by federal law enforcement, like the FBI. The explanation for this answer consists of the following analysis of the seventeen sections under Title II: Enhanced Surveillance Procedures that were incorporated into this case study analysis:

(1) It amended prior legislation to allow for FISA search and surveillance orders to be applied to terrorism investigations conducted by federal law enforcement.[27]

(2) It gave federal law enforcement the authority to intercept wire, oral, and electronic communications in investigations of terrorism and computer fraud and abuse offenses that target a wider range of crimes, such as: using chemical weapons & WMDs; violating criminal penalties under 18 USC 2332; committing acts of terror in foreign/international countries; providing resources/material & financial support to foreign organizations and operations; and engaging in financial transactions with foreign governments that support international terrorism.[28]

(3) It enabled federal law enforcement agencies, officers, and investigators to have matters involving foreign intelligence or counterintelligence or foreign intelligence information disclosed to them "only as necessary in the conduct of that person's official duties."[29]

(4) It authorized federal law enforcement to implement FISA surveillance methods such as "roving" warrants if they have cause to believe that the actions of the target of

[27] Section 201 of the USA PATRIOT Act of 2001
[28] Sections 201 and 202 of the USA PATRIOT Act of 2001
[29] Section 203 of the USA PATRIOT Act of 2001

their investigation may thwart/inhibit (make it more difficult to conduct) the surveillance of their actions.[30]

(5) It amended the Foreign Intelligence Surveillance Act of 1978 to extend the maximum duration of FISA search and surveillance orders applying for electronic surveillance and physical searches targeting both United States and non-United States persons.[31]

(6) It authorized federal law enforcement to use search warrants instead of wiretaps to obtain or "seize" voice-mail messages from a third-party communications service provider for investigative purposes.[32]

(7) It expanded the scope of subpoenas for electronic records by authorizing federal law enforcement agencies to require an internet service provider to disclose information about their customers including their name, address, telephone connection records/records of session times and durations, length and type of service used, telephone number/instrument number/subscriber number or identity/temporarily assigned network addresses, and credit card and bank account numbers; this provided federal law enforcement with the enhanced ability to conduct more thorough surveillance of a target.[33]

(8) It amended the Communications Act of 1934 to authorize cable operators to provide Federal law enforcement with a cable subscriber's records and "personally identifiable information."[34]

---

[30] Section 206 of the USA PATRIOT Act of 2001
[31] Section 207 of the USA PATRIOT Act of 2001
[32] Section 209 of the USA PATRIOT Act of 2001
[33] Section 210 of the USA PATRIOT Act of 2001
[34] Section 211 of the USA PATRIOT Act of 2001

(9) Under exigent circumstances, a provider of remote computing service or electronic communication service to the public may disclose to a federal law enforcement agency records or other personally identifiable information pertaining to a subscriber to or customer of such service(s) for investigatory purposes.[35]

(10) It authorized federal law enforcement to delay notifying a suspect that they have executed a search warrant targeting their persons or property, thus allowing them to extend the period of surveillance. It authorized Federal law enforcement 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" without providing immediate notification.[36]

(11) It amended the Foreign Intelligence Surveillance Act of 1978 to authorize federal law enforcement to use pen register and trap and trace surveillance to target both U.S. and non-U.S. persons for investigations aimed towards obtaining information relating to foreign intelligence or for investigations aimed towards protecting against international terrorism and/or clandestine intelligence activities.[37]

(12) It amended the Foreign Intelligence Surveillance Act of 1978 to authorize federal law enforcement to apply for an order allowing them to access and obtain "tangible things" like books, records, papers, and documents for their counterterrorism investigations.[38]

(13) It authorized federal law enforcement to apply ex-parte orders that would allow them to install their own pen register or trap and trace devices on a "packet-

[35] Section 212 of the USA PATRIOT Act of 2001
[36] Section 213 of the USA PATRIOT Act of 2001
[37] Section 214 of the USA PATRIOT Act of 2001
[38] Section 215 of the USA PATRIOT Act of 2001

switched data network of a provider of electronic communication service to the public" in order to electronically record any and all information collected from such devices for the purpose of collecting critical information pertaining to a criminal or terror-based investigation.[39]

(14) It authorized federal law enforcement to monitor, surveil, and intercept the communications of computer hackers.[40]

(15) It amended the Foreign Intelligence Surveillance Act of 1978 to authorize federal law enforcement to conduct surveillance in a terrorism investigation as long as the gathering of foreign intelligence information is the *significant* purpose—it no longer needs to be *the* purpose of the investigation.[41]

(16) It authorized federal law enforcement to execute a search warrant for property or for a person within or outside the district of application for the purpose of investigating domestic or international terrorism.[42]

(17) It authorized federal law enforcement to execute a search warrant for electronic evidence, thus allowing them to obtain a suspect's communications from a provider in any location across the country.[43]

The notion that the USA PATRIOT Act of 2001 impacted federal law enforcement's expansion of authorities by giving them too much leeway to investigate innocent Americans and unlawfully intercept their communications, thus violating civil rights and liberties, is unlikely;

[39] Section 216 of the USA PATRIOT Act of 2001
[40] Section 217 of the USA PATRIOT Act of 2001
[41] Section 218 of the USA PATRIOT Act of 2001
[42] Section 219 of the USA PATRIOT Act of 2001
[43] Section 220 of the USA PATRIOT Act of 2001

one study determined that, out of 21,248 claims filed between October 2001 and June 2013, only 265 were deemed credible and worthy of further investigation.[44] One of the main findings of this case study analysis was the identification of explicit "safeguard" clauses under the 17 major surveillance provisions of Title II: Enhanced Surveillance Provisions. In addition to Title II's newly enhanced surveillance provisions, there are numerous safeguards installed throughout the sections under Title II which prevent federal law enforcement from the misuse or illegal execution of FISA surveillance and searches. One example of a safeguard is the addition of a clause specifying that any federal law enforcement official who has information pertaining to a criminal or terrorism investigation disclosed unto them "…may use that information only as necessary in the conduct of that person's official duties subject to any limitation on the unauthorized disclosure of such information."[45] Another safeguard for the amended FISA pen register and trap and trace orders under Title II requires that the federal law enforcement may only use this amended FISA order for an investigation into foreign intelligence information or to prevent international terrorism and/or clandestine intelligence activities provided that such investigation does not violate the Constitutional amendments that enshrine the protection of civil liberties of citizens and residents of the United States.[46]

Part II. Limitations

Issues of reliability and validity almost always arise when conducting case study analyses. The most significant limitation to this thesis, with regard to issues of reliability and validity, is the time frame in which this case study analysis was conducted and developed. This

[44] Deflem & McDonough. (2015) Table 1
[45] § 203(a)(1)(C)(iii). *Pub. L. 107-56 (2001)*
[46] § 214(a)(1), § 214(a)(2), § 214(b)(1), § 214(b)(2). *Pub. L. 107-56 (2001).*

thesis was constructed over a six-month period and consisted of forming a proposal for thesis, defending the proposal, making edits, writing the remainder of the thesis, and then defending the final version. This particular case study analysis required a lengthy review process which largely extended the review period, leading to a time-constraint with regard to completing the analysis and finishing this thesis. Despite this, such a formal review of my case study was beneficial in that it enhanced the quality of the final version of this thesis by allowing for external, unbiased entities to review the content and provide helpful ideas, comments, and suggestions for revisions. A limitation to having a thesis committee oversee the development of my thesis is that they are the *only* audience. It may have been beneficial to have at least one more member on the committee.

Another limitation to this study resulted from an obstacle I faced when trying to conduct research for this thesis by gathering information about the USA PATRIOT Act of 2001 and terrorism in the United States through an online, scholarly journal database. The roadblock that inhibited the scope of my research was the inability to access a substantial number of sources that were relevant to the topic of federal law enforcement and their surveillance of terrorist activity. Some of the scholarly articles that I attempted to view and incorporate into my thesis were not able to be accessed unless you had authorization from a specific institution—Youngstown State University was not included as an authorized entity on certain journal articles. Some of the articles I tried to use were blocked, and the only way to override this was to purchase a subscription from the website's provider.

One limitation is the potential for future researchers to review this case study analysis and disagree with my conclusion that public confidence plays an influential role in the successful implementation and continued success of U.S. counterterrorism strategies, especially those

which concern the use of electronic surveillance by federal law enforcement agencies and investigators. This limitation also applies to those who disagree with Yin's model of case study methodology, which is the framework for the research conducted in this thesis.

Part III. Alternatives

If I were to do this study again, I would take a different approach to the case study analysis of the USA PATRIOT Act of 2001 by incorporating many of the other titles in addition to Title II, which served as the crux of this thesis. Some of the relevant titles I would have wanted to include if I were to repeat this study would be Title I: Enhancing Domestic Security Against Terrorism, Title IV: Protecting the Border, Title VII: Increased Information Sharing for Critical Infrastructure Protection, and Title IX: Improved Intelligence into my research because the provisions underlined within these sections are relevant to those in Title II: Enhanced Surveillance Procedures. An overarching concept present amongst these five titles under the USA PATRIOT Act of 2001 is the need to involve federal law enforcement in terrorism investigations. While these titles do not focus solely on surveillance procedures implemented by federal law enforcement agencies and investigators, which is the ultimate purpose of Title II, the concepts of increased surveillance and protection from terrorism are prevalent amongst them.

If I were to replicate this study, I would lengthen the literature review by incorporating more sources. Although fifteen scholarly articles and government publications were analyzed in Chapter 2, it would have benefited my case study research to include a larger and more diverse range of sources to represent the expansive nature of the USA PATRIOT Act of 2001.

An alternative approach to this case study, if I were to redo it, would involve the creation of an electronic case study database. The database I have developed for this thesis consists

primarily of physical documents; this inhibits the reliability of my case study methodology by making it difficult for a future researcher to replicate this study. Yin (2014) explains that case study data collection involves the creation of a formal database that contains all case study notes, documents, and data.[47] This database allows for the maintenance of a chain of evidence which is vital for producing a high-quality case study. Ultimately, my lack of an electronic database is a limitation to this case study because it diminishes the reliability of the research.

Part IV: Recommendations for Future Research and Policy Implications

A recommendation for future research into the USA PATRIOT Act of 2001 and its subsequent effect on terrorism in the United States is to analyze how the other titles impacted the way that federal law enforcement conducts surveillance. As mentioned in Part III of this Chapter, there were at least four other titles under the Act that were extremely relevant to this topic. Future researchers should incorporate at least one other title in addition to Title II: Enhanced Surveillance Procedures to ensure that the scope of analysis is as wide as possible. Titles I, IV, VII, and IX are the most relevant to federal law enforcement's surveillance of terrorist activity. The overlapping concepts must be explored in research into surveillance counterterrorism measures.

The most important policy implication to consider regarding the government's surveillance of terrorist activity, specifically that which is conducted by federal law enforcement, is the constitutional violation of civil liberties by governmental entities. A common misconception is that the government has too much power surrounding their ability to monitor and surveil the lives of innocent American citizens. Future counterterrorism policies must

[47] Yin, R.K. (2014). Case Study Research: Design and Methods. Fifth Edition, p. 105.

heavily consider strengthening and increasing the number of safeguard provisions with regard to federal law enforcement's authorities to conduct electronic surveillance in terrorism investigations; this is essential in reducing the likelihood of federal law enforcement engaging in unlawful surveillance procedures.

Another policy implication involves the general public's confidence in U.S. counterterrorism strategies. The literature review under Chapter 2 of this thesis provided articles which emphasized the importance of the public being involved in these strategies, albeit only to a certain extent. The scope of the public's involvement in U.S. counterterrorism strategies boils down to the degree of trust and confidence that American citizens place in federal law enforcement's implementation of surveillance procedures targeting terrorist activity. The implications of this case study on counterterrorism policy are extensive; government counterterrorism procedures are more effective and impactful if the public agrees with the strategies implemented. One of the underlying purposes of U.S. counterterrorism policy is to reduce the American public's perception of a vulnerable, unsafe nation. The expansive nature surrounding the USA PATRIOT Act of 2001's enhancement of government surveillance procedures only perpetuates the notion of the U.S. government using controversial, invasive or illegal practices. Future policies involving the surveillance of communications related to crimes of terror must consider public confidence as an integral component to the successful execution of counterterrorism strategies. Increasing the amount and quality of safeguard provisions regarding the government's implementation of counterterrorism surveillance procedures is essential in mitigating and eliminating terrorist threats.

Part V: Summary of Chapter and Explanation of Benefits

This Chapter presents this case study's major findings, limitations, alternative approaches, and recommendations for future research and policy implications. Now, the benefits of this research are discussed. A benefit of this thesis is its contribution to case study analyses in the fields of Criminal Justice and Homeland Security. This case study analysis of the USA PATRIOT Act of 2001 accurately encompasses Yin's (2003, 2014) description of case study methodology because its key design elements are represented throughout all five Chapters of my thesis. Chapter 1 provides an essential overview of the case study project[48] by giving background information about the 9/11 terror attacks and the passage of the USA PATRIOT Act of 2001; this chapter presents my research questions as well as the objectives for the following section. Chapter 2 involves a thorough literature review consisting of an analysis of 15 texts including scholarly articles and official governmental strategies; as mentioned previously, Yin (2014) emphasizes that the first part of a case study analysis is to conduct a thorough literature review. Chapter 3 introduces the initial propositions and explanations guiding this thesis. Chapter 4 provides an analysis and summary of the sections under the USA PATRIOT Act of 2001 which are then linked to the final theoretical propositions and explanations. This building of explanations to reflect my theoretical propositions is a specific technique for conducting a case study, which Yin (2003) believes to be crucial in producing a better, thorough, and more effective analysis.[49] Chapter 5 concludes the thesis by summarizing and discussing the previous chapters and major findings of the case study, the limitations of the study with respect to reliability and validity, alternatives for a replicate study, future research and policy implications, and the benefits of this thesis.

[48] Yin, R.K. (2003) Case Study Research: Design and Methods. Third Edition, p. 69
[49] Yin, R. K. (2003). Case Study Research: Design and Methods. Third Edition, p. 120

This thesis is beneficial to the field of Criminal Justice and future research into United States counterterrorism policies focused on protecting the Homeland because it resulted in a thorough case study analysis of Title II of the USA PATRIOT Act of 2001. The case study methodology provided for a complete breakdown of federal law enforcement's surveillance of terrorism in the United States. This technique facilitates a complete analysis of one of the most critical sections under the Act—Title II: Enhanced Surveillance Procedures. The provisions I analyzed in Title II are aimed directly towards enhancing federal law enforcement's access to investigatory tools in investigations of crimes of terror; these tools consist of electronic, mechanical, or other surveillance devices that are used to track and monitor a target under the scope of federal law enforcement's investigation.

The USA PATRIOT Act of 2001 was enacted with the intention of enhancing law enforcement investigatory tools for the purpose of deterring and punishing acts of terror that target the United States and its people. This Act expanded federal law enforcement's authorities with regard to conducting surveillance of terrorist activity in the United States through its amending of existing legislation including the Foreign Intelligence Surveillance Act of 1978, the Omnibus Crime Control and Safe Streets (the Wiretap Act) Act of 1968, and the Communications Act of 1934, resulting in one of the most significant and groundbreaking pieces of counterterrorism legislation.

References

9/11 Commission. (2004). The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. *9/11 Commission. Featured Commission Publications.* https://www.govinfo.gov/content/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf

Baldwin, T.E., Ramaprasad, A., Samsa, M.E. (2008). Understanding Public Confidence in Government to Prevent Terrorist Attacks. *Journal of Homeland Security and Emergency Management, 5*(1), 1-18 https://doi-org.eps.cc.ysu.edu/10.2202/1547-7355.1319

Baškarada, S. (2013). Qualitative Case Study Guidelines. *Joint and Operations Analysis Division: Defence Science and Technology Organisation.* https://apps.dtic.mil/sti/pdfs/ADA594462.pdf

Bellas, C. M. (2012). The USA PATRIOT Act of 2001: Legislative (In) Justice? *The Homeland Security Review: A Journal of the Institute for Law & Public Policy*

Brooks, B. E. (2010). Law Enforcement's Role in US Counterterrorism Strategy. *The Police Journal, 83*(2), 113-125. https://doi.org/10.1350/pojo.2010.83.2.480

CCR. (2002). Anthrax In America: A Chronology and Analysis of the Fall 2001 Attacks. *Center for Counterproliferation Research.* https://wmdcenter.ndu.edu/Portals/97/Documents/Publications/Articles/Anthrax-in-America.pdf

Cockfield, A. (2011). Surveillance as Law. *Griffith Law Review*, *20*(4), 795–816. https://doi.org/10.1080/10383441.2011.10854721

Deflem, M., McDonough, S. (2015). The Fear of Counterterrorism: Surveillance and Civil Liberties Since 9/11. *Society, 52*(1), 70–79. https://doi-

org.eps.cc.ysu.edu/10.1007/s12115-014-9855-1

Denniston, L. (2003). Arab Groups in US File Lawsuit Seeking to Curb Patriot Act. *The Boston Globe*, A3.

DHS. (2019). Department of Homeland Security Strategic Framework for Countering Terrorism and Targeted Violence. *U.S. Department of Homeland Security.* https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf

DNI. (2022). Strategic Intelligence Assessment and Data on Domestic Terrorism. *Director of National Intelligence. Federal Bureau of Investigation, Department of Homeland Security.* https://www.dni.gov/files/NCTC/documents/news_documents/2022_10_FBI-DHS_Strategic_Intelligence_Assessment_and_Data_on_Domestic_Terrorism.pdf

DOJ. (2004). Dispelling the Myths—The USA PATRIOT Act of 2001: MYTH VS. REALITY. *Department of Justice.* https://www.justice.gov/archive/ll/subs/add_myths.htm#s206

DOJ. (2023). The USA PATRIOT Act of 2001: Preserving Life and Liberty. *Department of Justice.* https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

Eller, W.S., Wandt, A.S. (2020). Contemporary Policy Challenges in Protecting the Homeland. *Policy Studies Journal, 48,* S33-S46 https://doi-org.eps.cc.ysu.edu/10.1111/pjs.12386

EPIC. (2023). Surveillance Oversight: PATRIOT Act. *Electronic Privacy Information Center.* https://epic.org/issues/surveillance-oversight/patriot-act/#:~:text=(Section%20216).,listen%20in%20on%20phone%20calls.

FBI. (2011). Domestic Terrorism: Focus on Militia Extremism. *Federal Bureau of Investigation.*

https://www.fbi.gov/news/stories/domestic-terrorism-focus-on-militia-extremism

FISC. (2023). About the Foreign Intelligence Surveillance Court. *United States Foreign Intelligence Surveillance Court*. https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court

Gonzales, A. R., Mueller, R. S. (2005). USA PATRIOT Act of 2001 Amendments to Foreign Intelligence Surveillance Act Authorities. *Federal Bureau of Investigation. Select Committee on Intelligence, United States Senate.*

Field, A. (2017). The Dynamics of Terrorism and Counterterrorism: Understanding the Domestic Security Dilemma. *Studies in Conflict & Terrorism, 40*(6), 470-483 https://doi-org.eps.cc.ysu.edu/10.1080/1057610X.2016.1221253

Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. 95-511. (1978). https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf#page=1

Hamm, M., Spaaj, R. (2015). Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies. *Office of Justice Programs.* https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf

LII. (2023). Definitions. *Legal Information Institute.* https://www.law.cornell.edu/wex/all

LII. (2023). U.S. Code: Table of Contents. *Legal Information Institute.* https://www.law.cornell.edu/uscode/text

Mabee, B. (2007). Re-imagining the Borders of US Security After 9/11: Securitisation, Risk, and the Creation of the Department of Homeland Security. *Globalizations, 4*(3). 385-397 https://doi-org.ysu.edu/10.1080/14747730701532567

Martinez, S. M. (2005). Testimony: Computer Provisions of the USA PATRIOT Act of 2001. *Federal Bureau of Investigation. Subcommittee on Crime, Terrorism, and Homeland Security Committee on the Judiciary U.S. House of Representatives, Washington, DC.* https://archives.fbi.gov/archives/news/testimony/computer-provisions-of-the-usa-patriot-act

NSC. (2021). National Strategy for Countering Domestic Terrorism. *National Security Council. The White House.* https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf

ODNI. (2018). National Strategy for Counterterrorism of the United States of America. *Officer of the Director of National Intelligence.* https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf

Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Act) Act of 1968, Pub. L. N. 90-351. (1968). https://transition.fcc.gov/Bureaus/OSEC/library/legislative_histories/1615.pdf

Roberts. (2005). Report 109-85. *Select Committee on Intelligence.* https://www.intelligence.senate.gov/publications/report-accompany-s-1266-permanently-authorize-certain-usa-patriot-act-provisions-june#:~:text=Simply%20put%2C%20Section%20202%20makes,an%20ordinary%20crime%20%60%60inextricably

Rackow, S. H. (2002). How The USA PATRIOT Act of 2001 Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of "Intelligence" Investigations. *University of Pennsylvania Law Review, 150*(5), 1651. https://doi-org.eps.cc.ysu.edu/10.2307/3312949

Sinha, G. A. (2014). NSA Surveillance Since 9/11 and the Human Right to Privacy. *Loyola Law Review, 59*(4), 861–946.

Swalwell, E.M., Alagood, R.K. (2021). Homeland Security Twenty Years After 9/11: Addressing Evolving Threats. *Harvard Journal on Legislation, 58*(2). 221-251 https://search.ebscohost.com/login.asps?direct=true&AuthType=ip,uid&db=a9h&AN=151357223&site=ehost-live&scope=site.

The White House Archives. (2001). Statement by the President in His Address to the Nation. *The White House Archives, President George W. Bush.* https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010911-16.html

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT OF 2001) Act of 2001, Pub. L. 107-56. (2001). https://www.govinfo.gov/app/details/PLAW-107publ56.

U.S. Department of State Archive. (2009). The Global War on Terrorism: The First 100 Days. *U.S. Department of State Archive.* https://2001-2009.state.gov/s/ct/rls/wh/6947.htm#

Wong, K. (2014). Exercising Jurisdiction Over Foreign Corporations: The USA PATRIOT Act of 2001 and the Extent to Which US Government Law Enforcement Agencies `Can Obtain Information from Abroad. *Communications Law Bulletin, Vol 33.2.*

Whitehead, J.W., Aden, S.H. (2002). Forfeiting Enduring Freedom for Homeland Security: A Constitutional Analysis of the U.S.A. Patriot Act & the Justice Department's Anti-Terrorism Initiatives. *The American University Law Review*, 51, 1081-1133.

The White House. (2001). Statement by the President in His Address to the Nation. *The White House Archives: President George W. Bush.* https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010911-16.html

Yin, R.K. (2003). Case Study Research: Design and Methods. Third Edition. *Sage Publications, Inc.*

Yin, R.K. (2014). Case Study Research: Design and Methods. Fifth Edition. *Sage Publications, Inc.*

Appendix

Definitions of Concepts and Terms

This section defines various terms and concepts frequently referenced throughout the USA PATRIOT Act of 2001 and this thesis: (1) international terrorism, (2) domestic terrorism, (3) federal law enforcement officer, (4) foreign intelligence information, (5) governmental entity, (6) foreign power, (7) agent of a foreign power, (8) what it means 'to engage in terrorist activity', (9) electronic surveillance, (10) wire and radio communications, (11) pen register & trap and trace devices, (12) adverse result, (13) 'ex-parte' order, and (14) computer trespassers and protected computers.

(1-2) 'Terrorism' is an umbrella term which covers two distinct natures of terrorist activity: domestic and international. Through 18 U.S.C. § 2331, the United States federal government has provided definitions of these terms. The main distinction between them lies in the jurisdiction in which the act of terrorism occurs. For instance, "…the term 'international terrorism' means activities that — (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished"; Domestic terrorism "(C) occur[s] primarily within the territorial jurisdiction of the United States…" (18 U.S.C. § 2331(5), 1992). More specifically, § 101(c) defines 'international terrorism' as activities

that consist of violent actions or acts that are considered to be harmful and/or dangerous to life that are also considered a violation of one or more criminal laws in the U.S.; such acts seem to be aimed towards the intimidation or coercion of a civilian population, the influence of government policy by intimidation or coercion, or the negative affecting of government conduct by means of assassinating or kidnapping (Pub. L. 95-511, 1978; Pub. L. 115-118, 2018). This description of the activities that coincide with international terrorism is also applicable to domestic terrorism.

(3) Under Title 18 of the United States Code, a federal law enforcement officer is defined as "…any officer, agent, or employee of the United States authorized by law or by a Government agency to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of Federal criminal law" (18 U.S.C. § 115(c)(1)). Examples of major federal law enforcement agencies are the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Department of Justice (DOJ), and the Department of Defense (DOD).

(4) Foreign intelligence information is defined in clause (iv) of § 203 (a) to cover the following: "…information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—(aa) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (cc) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of foreign power; or (II) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—(aa) the national defense or the security of the United States; or (bb) the conduct of the foreign affairs of the United States" (Pub. L. No. 107-56 2001).

(5) A governmental entity is defined in 18 U.S.C. § 2711(4) as any department or agency of the United States or any State or political subdivision thereof.

(6) As defined in § 101 under Title I of FISA (50 U.S.C. 1801), the term 'foreign power' is used to describe seven distinct properties.

I. A foreign government;

II. A faction of a foreign nation(s);

III. An entity openly recognized by a foreign government or a government that is directed and controlled by a foreign government(s);

IV. A group/organization/entity partaking in international terrorism or activities that coincide with preparing to commit an international terrorist attack;

V. A political organization whose origin is foreign-based;

VI. An entity being directed and/or controlled by a foreign government(s);

VII. An entity that is not composed of a majority of U.S. persons and is directly involved in the engagement of "international proliferation" of WMDS (weapons of mass destruction).

(7) 'Agent of a foreign power' is defined in § 101(b)(1) under Title I of FISA (50 U.S.C. 1801) and is a term applied to:

(A) any non-United States person that:

I. Is acting as an officer or employee of a foreign power in the United States, regardless of whether or not the person is physically in the United States;

II. Is acting in the United States for or on behalf of a foreign power that is engaging in clandestine activities which clash with the

various interests of the U.S., provided that the circumstances indicate that the agent may engage in such activities, or in the instance that the agent is knowingly and willingly aiding or abetting any other individual in the execution of such activities, or is knowingly conspiring with any individual to engage in such clandestine activities;

III. Is engaging in international terrorism, or activities in preparation thereof;

IV. Is engaging in the international proliferation of WMDs, or activities in preparation thereof, for or on behalf of a foreign power, or is knowingly and willingly involved in the aiding and abetting of another person engaging in such activities or those in preparation thereof or is knowingly and willingly conspiring with another person to engage in such activities, or activities in preparation thereof.

(B) any person that:

I. Is knowingly engaging in clandestine intelligence gathering activities either for or on behalf of a foreign power, in which such activities involve or might involve a violation(s) of criminal laws and statutes in the United States;

II. Is knowingly engaging, under the direction of a foreign power's intelligence service/network, in any other clandestine intelligence gathering activities either for or on behalf of a foreign power, in

which such activities involve or are about to involve a violation(s) of criminal laws and statutes in the United States;

III. Is knowingly engaging in sabotage, international terrorism, or activities in the preparation thereof either for or on behalf of a foreign power;

IV. Knowingly enters the United States with a false/fraudulent identity either for or on behalf of a foreign power, or knowingly assumes the wrong identity either for or on behalf of a foreign power while in the United States;

V. Is knowingly involved in the aiding and abetting of any individual in the execution of such activities described in these previous subsections.

(C) any person that knowingly conspires with any individual to engage in such activities described in the previous sections/subsections.

(8) It is essential to understand what it means 'to engage in terrorist activity.' Under Title IV: Protecting the Border, Subtitle B: Enhanced Immigration Provisions, there are six underlined actions which defines specific conduct that aligns with a clear intent to engage in terrorist activity. § 411. "Definitions Relating to Terrorism" states: "...the term 'engage in terrorist activity' means, in an individual capacity or as a member of an organization—

I. to commit or to incite to commit, under circumstances indicating an intention to cause death or serious bodily injury, a terrorist activity;

II. to prepare or plan a terrorist activity;

III. to gather information for potential targets for terrorist activity;

IV. to solicit funds or other things of value for—

i. (aa) a terrorist activity;

ii. (bb) a terrorist organization described in clause (vi)(I) or (vi)(II); or

iii. (cc) a terrorist organization described in clause (vi)(III), unless the solicitor can demonstrate that he did not know, and should not reasonably have known, that the solicitation would further the organization's terrorist activity;

V. to solicit any individual—

i. (aa) to engage in conduct otherwise described in this clause;

ii. (bb) for membership in a terrorist organization described in clause (vi)(I) or (vi)(II); or

iii. (cc) for membership in a terrorist organization described in clause (vi)(III), unless the solicitor can demonstrate that he did not know, and should not reasonably have known, that the solicitation would further the organization's terrorist activity; or

VI. to commit an act that the actor knows, or reasonably should know, affords material support, including a safe house, transportation, communications, funds, transfer of funds or other material financial benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training—

i. (aa) for the commission of a terrorist activity;

ii. (bb) to any individual who the actor knows, or reasonably should know, has committed or plans to commit a terrorist activity;

iii. (cc) to a terrorist organization described in clause (vi)(I) or (vi)(II); or

iv. (dd) to a terrorist organization described in clause (vi)(III), unless the actor can demonstrate that he did not know, and should not reasonably have known, that the act would further the organization's terrorist activity"

(9) Now, one must understand what the concept of "electronic surveillance" means since it is directly related to counterterrorism efforts in the United States, specifically those that involve the monitoring and surveillance of terrorist activity by federal law enforcement agencies, officers, and/or investigators. This term is defined in Ch 36: Foreign Intelligence Surveillance under Title 50: War and National Defense of the United States Code. Electronic surveillance encompasses the following components:

I. the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy, and a warrant would be required for law enforcement purposes;

II. the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United

States but does not include the acquisition of those communications of computer trespassers that would be permissible under 18 U.S.C. 2511(2)(i);

III. the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

IV. the installation or use of an electronic, mechanical, or other surveillance device in the U.S. for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes" (50 U.S.C. Ch. 36).

(10) Now that the concepts of electronic surveillance, wire communications, and radio communications have been explained, the acknowledgment of the specific devices used for these surveillance purposes is relevant to the study of surveillance procedures implemented by federal law enforcement in terrorism investigations. Examples of electronic surveillance technology includes, but is not limited to, cell phones that record geographic locations of users; RFID (radio frequency identification) tags in products that provide information regarding the location and usage of the products; video cameras; telephone and computer keystroke monitors; devices that can generate data regarding usage/performance of products; software programs that record IP (Internet Protocol) addresses (Cockfield, 2011). Wire communications are defined in § 1801(l) under Chapter 36: Foreign Intelligence Surveillance in United States Code Title 50: War and National Defense as any type of communication that is carried by a wire, cable or other

apparatus and being supplied by or controlled by any individual who serves as a "…common carrier in providing or operating such facilities for the transmission of interstate or foreign communications" (50 U.S.C. Ch. 36. § 1801(l)). Radio communications are defined in Title 47 of United States Code under § 153 as the "transmission by radio of writing, signs, signals, pictures, and sounds of all kinds, including all instrumentalities, facilities, apparatus, and services…incidental to such transmission" (47 U.S.C. Ch. 5. § 153).

(11) Section 3127 under title 18, United States Code, provides definitions for the terms 'pen register' and 'trap and trace device,' which are important to understand with regard to federal law enforcement's surveillance of terrorist activity in and outside of the United States. A pen register is a technical device or process that is able to record and/or decode information and data related to dialing, routing, addressing, or signaling that is transmitted via an instrument or operations facility that is involved in the transmission of wire and electronic communications (18 U.S.C. 3127(3)). A trap and trace device is a sophisticated instrument or process that is capable of receiving and capturing an influx of electronic impulses (and other types) that are helpful because they can identify the targeted number and other information related to dialing, routing, addressing, or signaling that may be able to locate the source of the transmission of wire or electronic communications (18 U.S.C. § 3127(4)).

(12) An 'adverse result' is defined in § 2705(a)(2) and is, in essence, an unwanted action or outcome. For the purposes of § 2705 "Delayed notice', an adverse result refers to the possible effect(s) of the target of a search warrant being immediately notified of the execution of such warrant. These effects lead to the following adverse results: (a) endangering the life or physical safety of an individual, (b) flight from prosecution, (c) destruction of or tampering with

evidence, (d) intimidation of potential witnesses, or (e) otherwise seriously jeopardizing an investigation or unduly delaying a trial (18 U.S.C. § 2705(a)(2); LII, 2023).

(13) An 'ex-parte' order is defined as a motion (formal request for a desired ruling, order, or judgement) for an order (court's decision) that is able to be granted without having to wait for the other party to respond (LII, 2020; LII, 2022; LII, 2023).

(14) Computer trespassers and protected computers are concepts related to § 217 "Interceptions of Computer Trespasser Communications." 18 U.S.C. § 2510(21) defines a 'computer trespasser' as someone who accesses and uses a protected computer without the required authorization to do so.

18 U.S.C. 1030(e)(2) defines a 'protected computer' as one that is:

I. solely for the purpose of being used by or for a financial institution or the United States Government;

II. being used in or is affecting interstate or foreign commerce or communication, including a computer used outside of the U.S. in such a manner that ultimately affects those entities of the United States;

III. a part of a voting system; used for management, support, or administration of a federal election; moved in or otherwise affects interstate and/or foreign commerce.