U.S. Surveillance of Citizens:

The Prevention of Domestic Terrorism

David A. Rogers

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2019

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
fulfillment of the requirements for graduation from the
Honors Program of Liberty University

Joel Cox, Ph.D.
Thesis Chair

Stephen Parke, J.D., L.LM.
Committee Member

Christopher Jones, Ed.D.
Committee Member

Emily C. Knowles, D.B.A.
Assistant Honors Director

Date

Abstract

The United States drastically increased the powers given to the federal government following the terrorist attacks of September 11, 2001, as the sheer number of casualties and shock that struck the nation called for an immediate response. The fear of another mass attack is still within the minds of the American people, and the U.S. government has taken measures to attempt to prevent such a tragedy. This thesis will analyze the topic of domestic surveillance, as well as ethical concerns for the criminal justice field, and will explore the future of homeland security and anti-terrorism for this country if this trend of surveillance continues.

U.S. Surveillance of Citizens:

The Prevention of Domestic Terrorism

When the nation witnessed the Twin Towers of the World Trade Center collapse with thousands of innocent victims trapped inside, the threat of a terrorist attack on American soil was realized. The perceived "invulnerability" of American security and safety from terrorism on the mainland was shattered, and the U.S. government set forth a series of new anti-terrorism methods that have changed the government's approach to homeland security as it seeks to prevent another such attack. Although these measures seek to protect the citizens of the United States, the surveillance and other security methods used, such as the PATRIOT Act and state fusion centers, also carry ethical concerns for criminal justice professionals and could potentially have a huge impact on the future of homeland security in the United States.

A New Era of Security

While the United States certainly had security measures implemented to try and ensure the safety of its citizens and agencies working to seek out dangerous individuals and groups prior to the terrorist attacks of 9/11, the legislation and policies that followed began a new age of approach to homeland security measures. Almost immediately after the attacks, President George W. Bush signed into law one of the most controversial pieces of legislation, the USA PATRIOT Act, which stood for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act." This legislation gave the federal government unprecedented freedoms and powers to investigate and monitor the lives of its citizens, as many government officials were either too afraid of another attack or willing to justify the loss

of privacy rights in the name of security to fully comprehend the effects this Act would have on the lives of American citizens (American Civil Liberties Union [ACLU], n.d.). Not only was the power of the federal government and executive branch enhanced, but law enforcement agencies as well experienced a new sense of control after the September 11th attacks. Dahl (2011) wrote, "at least 263 government agencies and organizations had been created or reorganized as a response to 9/11" (p. 3). This surge of new legislation and security organizations has ushered the American people into an era of government surveillance and monitoring, most of which is conducted during nonemergency situations.

Domestic monitoring was certainly ongoing before the terrorist attacks on the World Trade Center and the "war on terror" began, as is evident by the formation of the Church Committee. The Church Committee was formed after journalist Seymour Hersh publicized an article claiming the CIA had abused their intelligence responsibilities by conducting surveillance on anti-war activists, leading to a call for a congressional inquiry (U.S. Senate, n.d.). It was tasked with investigating the nation's intelligence agencies and found that intelligence excesses had begun during Franklin Roosevelt's administration and continued on through the early 1970s (U.S. Senate, n.d.). However, homeland security organizations and officials have been developing further methods and implementing these new ideas in order to monitor those residing in the United States and their communication with potential terrorist groups or individuals. Monahan (2010) wrote, "state surveillance has grown and mutated in response to changing perceptions of the nature of terrorist threats" (p. 84). The Department of Homeland Security has actively been establishing "fusion centers" around the country. These fusion centers analyze data

on citizens and conduct counterterrorism methods, such as roving wiretaps, based on this data, essentially targeting individuals that "match certain profiles and singles them out for further monitoring or preemptive intervention" (Monahan, 2010, p. 84). Far from being inactive, the government and its various agencies, like the DHS and the FBI, have pushed further into the realm of intelligence and surveillance, even to the point of overstepping the legal bounds and rights to privacy that the Constitution and federal policies ensure, as Lewis found that evidence existed of terrorist attacks being the basis for passing existing agendas and expanding government authority at the cost of individual civil liberties (2005, p. 26).

The world of counterterrorism is a very private and isolated realm, but many Americans are still uninformed of the danger that presents itself to the agencies who are tasked with protecting them. According to Zwerman (1989), "Most Americans continue to associate 'terrorism' with well-publicized incidents that occur outside the U.S. and understand 'counterterrorism' as a policy that affects certain insurgent groups in the Third World and Western Europe" (p. 34).

While there has not been another tragedy that has compared to the World Trade Center massacre, numerous attacks and deaths have received attention in the United States, such as the shooting in San Bernardino, California in 2015, and the nightclub shooting in Orlando, Florida, in 2016. In San Bernardino, a Pakistani couple opened fire on a company training event and Christmas party, after being radicalized through online propaganda; as for the Orlando shooting, a young Muslim man killed dozens at a nightclub, citing his allegiance to ISIS and revenge for American bombings in the Middle East as his motivation (Rokos, 2016).

It is only in recent times that the possibility of a terrorist attack is becoming more of a reality for Americans, as Islamic extremist and radical right-wing groups, as well as individuals inspired by jihadist teachings and propaganda online, have begun to make their efforts more well known. New technology, biological weapons, and improvements on bombs have increased the avenues for potential targets, leading to an increase in national attention and creating more opportunities for attacks (Black, 2004, p. 22). In order to accommodate the growing vulnerabilities of American society, homeland security organizations must be continuously evaluating their current measures and seeking to implement additional measures to best protect the public. However, the balance between security and protecting personal liberties is constantly being called into question, as the U.S. government has struggled with in the recent years concerning unconstitutional domestic surveillance measures.

Counterterrorism and Recent Developments

The United States has been at the forefront of fighting back against terrorism, so much so that almost any major attack or mass tragedy is labeled as an "act of terrorism" by Americans who have been so indoctrinated by the media that they believe mass death is a certain sign of terrorism. Powell (2011) analyzed media reactions to terrorist attacks in the United States and found that "Immediate coverage of each act defined the act as terrorism and agent as a terrorist. Words such as domestic terrorist or terrorist were used, even before the act was established by investigators as terrorism or any arrest was made" (p. 98). While terrorism is not to be taken lightly, it is also crucial to be aware of the danger of over-preparing and cautiousness, as this can cause a normal functioning society to become authoritarian and restricting personal liberties and freedoms in a well-meaning

attempt to curb individuals and groups from making their statements through violence. While clearly not all of the security measures are made known to the public and thus cannot be discussed in this paper, it is important to attempt to create as clear a picture of the security that is in place as possible in order to more knowledgeably discuss the ethics and controversies surrounding counterterrorism and domestic surveillance.

Arguably the most famous piece of legislation that arose from the aftermath of the September 11th attacks is the controversial USA PATRIOT Act, signed into law by President George W. Bush. This legislation revised several standing statutes that dictated regulations for surveillance and counter-terrorist intelligence, broadening police capabilities with respect to surveillance and monitoring, including the use of roving wiretaps to follow targets rather than specific objects like a phone, and broadening the scope of "pen register" and "trap and trace" devices which follow telephone and computer IP addresses (Bloss, 2007, p. 215). While perhaps some areas of this legislation do not infringe on privacy or are even improvements to existing policy—namely the lowering of the standard to which pen/trap orders can be ordered, possibly saving the government from having to seek excessive intercept orders—civil rights advocates nevertheless protest about the lowering of privacy standards and intrusion of constitutional rights (Henderson, 2002, p. 200). Thus, police and government agencies were granted new abilities and expanded powers to conduct warrantless surveillance on United States citizens or other residents, as the Terrorist Surveillance Program enabled the NSA to expand its scope. This expansion of federal power exhibits the exact cause for fear that civil rights advocates have, as they see the growing responsibilities and abilities

to conduct surveillance as legal ways for the government to restrict citizens' privacy rights and spy on them without warrants.

One of the controversial counterterrorism measures that President George W. Bush enacted after the September 11th attacks was the Terrorist Surveillance Program. This program allowed the National Security Agency (NSA) to monitor and intercept emails and phone calls that were travelling into and from the continental United States outside of the legal parameters that the Foreign Intelligence Surveillance Act, or FISA, has set for electronic surveillance of persons suspected of terrorism or being involved in terrorist activities, which understandably has generated conflict among those who are proponents of individual liberties (Yoo, 2007, p. 566). Such monitoring of electronic transmissions certainly raises the question of invasion of privacy and civil liberties that are guaranteed in the Constitution, showing just how far the American system of defense against terrorism has come in just a few short years. Although it has since been replaced, its essential elements of monitoring and surveillance are still active in the program code named PRISM that replaced it.

Economic sanctions and policies that affect the assets and revenue of countries, organizations, and individuals that support or are affiliated with terrorism are also in place and at the disposal of the President to enact. The International Emergency Economic Powers Act allows the President to impose regulations and restrictions on economic relations, as well as regulating all financial transactions like the transferring of funds and credit between the United States and the country sanctioned (Perl, 2001, p. 7). While this security measure can be considered more of an international policy as opposed to a domestic measure, it still can still have effects on those individuals or groups

operating within the United States, as funds or support can be cut off to stop future attacks or planning. Economic sanctions can only do so much against terrorism, however, as terrorist organizations have multiple ways of revenue for their funding and cannot always be enforced internationally. Perl (2001) stated, "Sanctions usually require the cooperation of other countries to make them effective, and such cooperation is not always forthcoming" (p.7). These sanctions do serve as a diplomatic and public step in denouncing that country in the hopes that other countries may perhaps also follow suit and cut off support, as Perl cited several U.N. measures that required members to freeze assets and deny support to terrorists (p. 6).

As mentioned previously, the creation of "fusion centers" is one of the most recent developments in the counterterrorism atmosphere, as the Department of Homeland Security sought to create a network of information and data sharing throughout the nation so that profiled individuals and groups could be monitored more efficiently and with greater ease. Similar to the FBI's "Joint Terrorism Task Force" (JTTF) programs, these fusion centers expanded on such roles and responsibilities and incorporated a more all-encompassing approach to hazards and threats as well as terrorism, and monitor data and intelligence to assess threats and risks to the United States rather than actively monitoring or conducting surveillance on persons and their property (Monahan, 2010, pp. 85-86). These fusion centers have the immense task of analyzing data from multiple sources including social media, financial records, and other online intelligence that helps to build a profile and risk assessment for individuals and organizations, while balancing the privacy of such people and attempting to prevent target profiling or discrimination based on one's religion, race, or any other filter that deviates from whatever standard authority

has set (Bernal, 2016, p. 258). In a society that runs on technology, fusion centers highlight the importance of data surveillance, as "imperatives to collect, share, analyze, and act on data increasingly shape the activities of public institutions, private companies, and individuals" (Monahan, 2010, p. 94).

Recent advances in homeland security over the last several years are bringing attention to the continuously growing federal and state intelligence agencies and organizations designed to aid the Department of Homeland Security in all matters of defense, not just terrorism. Dahl (2011) discussed the creation or recent growth of agencies, such as the National Counterterrorism Center and the El Paso Intelligence Center (EPIC), which serve to help coordinate efforts and intelligence against threats to the nation and utilize the intelligence and data that is available to them in order to best assist law enforcement and other government agencies (p. 4). Zwerman (1989) correctly theorized that the domestic counterterrorism program would continue to expand in the United States and broaden the definition of who may be included within the "terrorist" phrase to individuals like "terrorist supporter" or "potential terrorist" (p. 58). As the threat of acts of violent terrorism grows and other nations experience a rising number of attacks from jihadists or other individuals seeking to make their statement known, the United States is continuously adding to its defensive measures and expanding the size and responsibilities of the counterterrorism agenda in order to keep its citizens safe and to attempt to prevent these future attacks from occurring.

The Age of Information Sales

In today's world where technology, social media, and electronics control societies and form the foundation for many aspects of a culture, people's identities and private

information are entered into countless websites and accounts, whether for a social media page like Instagram or Twitter, an email account run by Google or Yahoo, or an online banking account for Wells Fargo or Bank of America. In 2016, Bernal wrote

> People use the internet to establish and support personal relationships, to find jobs, to bank, to shop, to gather the news, to decide where to go on holiday, to concerts, museums or football matches. Some use it for education and for religious observance– checking the times and dates of festivals or details of dietary rules. There are very few areas of peoples' lives that remain untouched by the internet. (p. 253)

The online presence of just one single individual in America is immense, and brings greater chances for being hacked or their information stolen with every additional account opened or information entered. This information that is entered into one website does not simply stay locked away; rather, this data is collected, sold, and distributed to dozens of data brokers, who use this information to create precise profiles of individuals and then sell this information to advertisers and marketers to use in their ploys to sell products and services to these individuals (Goodman, 2015, pp. 66-67). This profiling by such companies to ensure better sales poses a serious threat to the privacy of individuals, as well as crossing into a new world of legality. While this information and online profiles can be put to good use, such as for background checks and inspection of social media posts for law enforcement agencies to ensure that an individual was not an active promoter of terrorist agendas, it still creates an issue of privacy as an individual can no longer expect reasonable privacy with regards to online posting or activity.

Not only are private companies enjoying the benefit of data and information people so readily input online, but the government and law enforcement agencies can now reap the benefits of access to personal online data, such as the aforementioned social media searches for background checks. However, the government also can subpoena companies, like AT&T, for information in civil and criminal cases without breaking the Fourth Amendment through the third-party doctrine. Goodman (2015) wrote, "What data…the government doesn't subpoena, it just buys. The NSA and other government agencies…purchased or otherwise obtained a complete copy of what the corporate world was already collecting" (pg. 78). Corporations and companies are realizing the financial gain that can be obtained by selling information to the government, and allowing access to federal agencies is becoming the new norm for the private sector (Giroux, 2015, p. 111). While this presents a great opportunity for companies and the government to both benefit and profit from this data, the ethical dilemmas that accompany these furtive purchases carry huge implications for criminal justice professionals and the general public as well.

Domestic Surveillance and Ethics

As domestic surveillance and monitoring measures expand and continue to incorporate new technology to accommodate the growing threats and avenues for terrorism, it is essential for criminal justice professionals to consider and discuss the ethical implications that such practices carry, as well as the legal controversies they create in regards to the rights guaranteed in the Constitution. As Edward Snowden revealed, the NSA conducted warrantless surveillance and monitored thousands of people's personal information and electronic data in attempts to gain data and increase

the global security community's intelligence network, regardless of privacy rights or the legality of such actions, as Snowden said "NSA and intelligence community in general is focused on getting intelligence wherever it can by any means possible" (Landau, 2013, p. 54). In order to protect the integrity of the Constitution on which the United States was built, there must be a system of accountability that must be enforced in order to prevent the government from overstepping its boundaries, and yet it is crucial that privacy is maintained so that not all of the government's security measures are made public and known to enemies of the county and its ideals. This balancing between privacy and personal liberties against security is an ever-present conflict within the criminal justice world, as two different priorities must be considered while designing new policies and legislation, creating a struggle for dominance of criminal justice professionals' decisions.

Privacy versus security debates are difficult for officials to determine the correct option because the discussion revolves around two important and essential aspects of any legislation, as they must seek to ensure the safety and protection of citizens and yet must also consider these individuals' rights to privacy and freedoms guaranteed in the Constitution that protect them from certain instances of unwarranted surveillance and monitoring without their knowledge. Laidey (2015) asked, "Is it really fair or just to undermine the privacy of millions of otherwise innocent users, to seek out a few criminals and/or terrorists?" (p. 2237). Ethically speaking, it becomes difficult to determine a "right" option in these debates, as arguments can be made in support of either side and its benefits to society, and both seek to protect the citizen, albeit in different ways. Those in the criminal justice world are constantly forced to determine where their own individual morals and sense of ethics lie and wrestle with the policies and legislation

that are brought to their attention every day, as it is different for each person where the line of legality and ethically correct practices fall. These decisions must be made constantly in the world of counterterrorism and surveillance, and carry consequences that may drastically affect the world of criminal justice in the future, as the NSA discovered when Snowden revealed their surveillance practices for the world to see.

The Constant Debate of Privacy Versus Security

No matter what the area of criminal justice, there will always be a debate between personal liberties and security, as these two principles constantly clash. Finding a proper balance between the two is what criminal justice professionals are seeking to do every day, as upholding the Constitution and the rights it guarantees is essential, but ensuring the safety of those living in America must also be a top priority and certainly is. After the September 11th attacks, in the midst of public terror and panic, the federal government leapt at the opportunity to expand upon its power and enhanced the practices of law enforcement and other federal agencies in order to create as secure an environment as possible. More intensive screenings at airports and other public transportation spots by the TSA, authorization of the search or surveillance of individuals without the approval of a judge or court, and greater freedom for FBI agents to conduct investigations and surveillance without warrants are all examples of the government's expansion of its own power at the expense of personal liberties (Dahl, 2011, pg. 5).

One of the earliest measures enacted that is designed to protect citizens from unnecessary and unwarranted surveillance by federal agencies and intelligence organizations is the Foreign Intelligence Surveillance Act, better known as FISA, which establishes procedures and guidelines for the surveillance and intelligence gathering of

information between foreign powers and their agents, whether on foreign soil or domestic. This Act established a court specifically designed to review applications for electronic surveillance that required agencies to show probable cause for the targets being foreign powers or agents of foreign powers (Henderson, 2002, p. 192). As mentioned previously in the paragraph discussing counterterrorism measures, the Patriot Act lowered the standards to which law enforcement can obtain surveillance orders and conduct warrantless surveillance, undermining the FISA court's ability to limit intrusion and creating more opportunities for intelligence organizations to circumvent FISA's standards.

As the issue of unwarranted searches and surveillance has constantly surrounded law enforcement, the Supreme Court has made several rulings in the debate of privacy. In *Katz v. United States*, the Supreme Court found that the Fourth Amendment protection extends to anywhere that an individual may have a "reasonable expectation of privacy," as Justice Stewart wrote "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth, and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment" (*Katz v. United States*, 1967). As several decades have passed since that decision, the Supreme Court has also struggled with adapting the *Katz* ruling to the technological advances made in society, as evidenced by *United States v. Jones* (2012) and *Riley v. California* (2014), which dealt with police utilizing a GPS device to track vehicle movement and the warrantless seizure and search of a cell phone during an arrest, respectively, both of which the Supreme Court decided in favor of extending the individual's privacy. In 2018, the Supreme Court in a 5-4 decision found

that the obtaining cell-phone records that provide a log of an individual's location constitutes a search under the Fourth Amendment, as Chief Justice Roberts wrote,

> In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. (*Carpenter v. United States*, 2018)

As shown through these cases, the Supreme Court is attempting to protect the Fourth Amendment rights guaranteed to citizens and limit the federal power for searches and surveillance. However, the *Carpenter* case shows how difficult it is for the justices to adapt to the growing technological advances and determine what is protected under the Fourth Amendment.

However, some scholars and individuals believe that the growing security and surveillance measures are an important step in keeping the country safe and ensuring that those who intend to do harm to others are stopped before the actions are taken. Yoo (2007) said, "In this world of rapidly shifting e-mail addresses, multiple cell phone numbers, and internet communications, FISA imposes slow and cumbersome procedures on our intelligence and law enforcement officers," (p. 576) as he believes that the policies in place are "looking backward in order to conduct prosecutions of those who have perpetrated crimes or infiltrated the government, rather than operating within the national security system, which looks forward in order to prevent deadly surprise attacks on the American people" (p. 576).

Herein lies the problem: there is no definite stopping point for the government expanding its power to ensure security. There is no fixed point along the scale of expansion that is deemed "too much power" until it is too late to go back, and the government becomes authoritarian, holding the power and limiting the freedom of the people. In his 2015 article, Giroux wrote,

> As the line between authoritarian power and state governance evaporates, repression intensifies and increasingly engulfs the nation in a toxic climate of fear and self censorship in which free speech, if not critical thought itself, is viewed as a practice too dangerous in which to engage. (p. 124)

George Orwell in his novel *1984,* wrote about an omnipotent government state who subjected its citizens to constant surveillance in order to curb any individual thinking or privacy that could spark rebellion (1949, pp.1-328). While perhaps the United States has not reached this drastic point of government control, it certainly is on the way to becoming this authoritarian form of government if some actions to curb government surveillance and monitoring are not taken in the future, as individuals' privacy rights are shrinking and the judicial and legislative branches appear to be leaning in favor of consolidating power in the central government. Bloss (2007) stated, "Therefore, the identities, transactions, and movements of citizens are less private and more accessible to police through burgeoning databases of personal information; all derived from official surveillance and search activities" (p. 222).

On the other side of the scale, ensuring personal liberties and freedoms must also remain a goal for criminal justice professionals, as the Constitution dictates the rights of speech, privacy, religion, and others like them so that this country can be unique and

embrace differences in individuals. Protecting the public goes beyond simply ensuring their physical safety and well-being; rather, this duty also extends to protecting the rights and principles for which these people also hold and trying to protect their right to have their own distinct beliefs and opinions, even if those beliefs and opinions are contrary to law enforcement goals, or the officer's individual worldview. Even as most citizens are unaware or simply complacent towards the new steps and measures taken in the name of national security, it does not give law enforcement and federal agencies the right to continue to push the boundaries of what is considered constitutional and legal and further diminish the privacy given to citizens. "Rarely do citizens acknowledge the prospect of drastic political and social transformation, making it difficult for them to appreciate the dystopian potentials inherent in certain technologies" (Haggerty & Gazso, 2005, p. 184). Taking advantage of the public's general ignorance or lack of understanding is not what criminal justice professionals should seek to do, nor should the public be left uninformed about the government's actions or intent.

The role of the government in such privacy matters must be in service to the public, not to better support the power and importance of itself, as this goes against the nature of the Constitution and the foundation on which the country was built through democratic principles; "We the People" are the sovereignty. National security and the protection of those who are living in America is clearly essential, and citizens must understand that there will always be conflict between their own personal liberties and their safety. Some compromises must be made, as no solution will be able to fully satisfy all individuals' beliefs and the government's needs, and it is important for the government to respect the privacy rights that are included in the Constitution. However,

the federal government in recent years has taken such decisions and given itself more power at the expense of privacy and personal liberties, and discretion is left up to the executive and legislative branches about what are adequate security measures. Henderson (2002) wrote, "Thus, where executive power has increased, as it has here, Americans should be concerned that privacy may be unnecessarily threatened as a result" (p. 208). Even as some measures try to meet a middle ground, such as some provisions of the Patriot Act seek to do, most of the legislation and policies that have been enacted in recent years are in favor of expanding the power of government surveillance and allowing further intrusion into individuals' lives.

The furtherance of government surveillance and expansion of federal power has led to an outcry from some individuals and organizations, like American Civil Liberties Union (ACLU), who take action when they feel that the government has overstepped its bounds and violated the personal rights and liberties guaranteed in the Constitution (ACLU, n.d.). The enhancement of police surveillance parameters and federal power into monitoring and profiling American citizens has serious effects on society, as it causes individuals to undergo surveillance and unnecessary intelligence gathering simply to satisfy the government's attempts to cut off all threats from forming into decisive action. America's law enforcement surveillance society has seen a change from detecting crime for the use of evidence to the preventative idea of gathering intelligence on potential threats and individuals before the action is taken or the individual is actually revealed to be dangerous (Bloss, 2007, p. 210).

This shift of thinking in law enforcement and proactive approach to surveillance has caused a great amount of unrest and concern within the civil liberties community, as

the fear of privacy invasions and civil liberties violations comes to the forefront of their perspective of society and where it is heading in the future. In 2004, Martin said in her article,

> There is every reason to fear that the Administration's insistence on describing the domestic counterterrorism task as an 'intelligence' one is a back door effort to…allow the use of 'intelligence' and military methods against individuals…found in the United States and fully protected by the Constitution. (p.13)

However, it is also important for the civil liberties community to also realize the importance of security and not overreact to the growing government surveillance presence in their lives, as there still are legal safeguards and policies that are designed to limit the government. "The culturally embedded assumption that surveillance is powerful and harmful to rights and liberties, which is also sustained by claims-making by surveillance scholars and activists alike, may drive civil liberties allegations independent from actual violations thereof" (Deflem & McDonough, 2015, p. 78). Caution and safeguards must still remain in order for this society to not turn down a path towards authoritarianism, but there must also be a sense of security and safety that must come into conflict with privacy. Nevertheless, the American public still hold their privacy rights and civil liberties dear and stand in support of enforcing those rights. Lewis (2005) wrote,

> As they shape legislation and design regulations, prudent political and administrative leaders will remember that Americans cherish the idea of civil liberties…Moreover, a majority of Americans reject the proposition that a sacrifice of civil liberties is necessary to fight terrorism. (p. 26)

While safety is considered important to Americans, many are unwilling to give up their civil liberties and think that sacrificing them in the name of more security is not worth the expense. At one time, public opinion may have been in favor of expanding government power, but it has once again shifted back after the threat of immediate terrorist attacks such as 9/11 is no longer considered to be an urgent danger.

Ethical Concerns for Surveillance

As technology becomes increasingly essential to American society and is further integrated into every aspect of daily life, more and more opportunities for threats to the United States continue to grow. With the rise of technology, the government has been forced to update its ways of monitoring dangerous individuals and organizations, as now they have numerous avenues of communication and transactions that cannot be easily followed by federal agents or law enforcement officers. However, this increase of surveillance measures and legislation that limits privacy rights has stirred up civil liberties' activists, and should be a point of concern from the American public and law enforcement officers alike. Not only does this bring into question the range of the Constitution's protection, but also challenges individual federal agents and law enforcement officers concerning their moral beliefs. Policy makers are also forced to question their ideals and principles, as they are the ones who must determine what new measures should be enacted and what further details must be added in order to ensure the safety of the nation.

One area of ethical concern that must be addressed is the issue of discrimination and profiling when it comes to targets of surveillance, whether it is based on race, religion, political beliefs, or participation in various protests or other such activities.

Monahan (2010) discussed some of the controversies that fusion centers and their assessments of individuals have been involved in, such as the investigations by the Maryland State Police of anti-death penalty activists and peace activists even though there was no indication of violent activities by the members, who were listed in federal databases as being suspected of "terrorism—anti-government" (p. 89). When assembling profiles of individuals or organizations who may pose the biggest threat to the nation, it can be easy to focus too much on those who deviate too far from the social norms and threaten to upset the status quo.

Surveillance should be based on factual data and observable cause for concern and safety threats, not simply because they share the same religion of previous terrorists or because they are the same race. "As Norris and Armstrong (1999) have shown in their ethnographic study of CCTV systems, camera operators employ a host of highly stereotypical and questionable markers related to a citizen's age, race, clothing and demeanor to identify individuals deserving special attention" (Haggerty & Gazso, 2005, p. 182). When establishing targets for surveillance and assessing threats, it is crucial for law enforcement officers and federal agents to be conscious of their biases and make objective decisions to determine those most likely to bring danger to the country, and to not discriminate against a certain race or religion without cause for surveillance.

A second ethical concern when discussing domestic surveillance is the clear overstepping of privacy rights and expansion of government authority. Because the American public has not fully understood the implications of government surveillance or simply are unaware of the practices, the government and policy makers have taken advantage and created a new domestic intelligence system that has pushed the limits on

individual privacy and upsetting the balance of security and liberty in even greater favor of security. Law enforcement officers and federal agents must consider whether or not they believe that this surveillance conflicts with innocent people's rights to privacy, and if the massive collection of data and surveillance of innocent people conflicts with the freedoms in the Constitution. Martin (2004) discussed the importance of proper focus for intelligence agencies, saying that they must "focus on criminal activity, which encompasses all terrorist plotting and financing, rather than authorizing an intelligence approach that absorbs all available information about thousands of individuals in the hope of finding something useful" (p. 11). For some scholars and civil liberties activists, finding a cause for the surveillance and intelligence gathering should be the standard for the invasion of privacy and further monitoring.

However, other scholars argue that such a limited approach and individualized suspicion is counterintuitive to the preventative nature of counterterrorism and express their belief in the power of intelligence gathering on a broad scale. Yoo (2007) wrote, "The purpose of the criminal justice system is to hold a specific person responsible for a discrete crime that has already happened. By contrast, the purpose of intelligence is to guide actions…that prevent future harm to the nation…" (p. 583). Intelligence is not meant to follow the same rules as law enforcement standards, as intelligence is a tool with which to gain information about threats before they can materialize. "The U.S. government should therefore have the authority to monitor any group and its potential state sponsors that might have the motive and the means to use weapons of mass destruction" (Carter, Deutch, & Zelikow, 1998, p. 83). As shown here, some scholars hold this belief that the importance of surveillance and a broad domestic intelligence

program is necessary for the safety of American citizens because the intelligence system is not designed to be similar to the criminal justice system and be used as a way to punish offenders who have already committed a crime, but as a weapon against the plans of terrorists.

The author of this thesis believes that a balance of the two approaches must be taken, as the intelligence community should be given more freedom than law enforcement officers and yet should still be held accountable for the information and data they collect on individuals. Not only should responsibilities be specifically stated and detailed, but also a more proactive oversight system should be created or tasked in order to prevent abuses. However, in the interest of national security, the author believes that erring on the side of security is a necessary risk that must be utilized in order to keep innocent civilians safe from terrorist attacks. This should not be the standard, but should be done with careful oversight in order to ensure that abuse and unlawful surveillance are avoided when there is no threat or a threat has been mitigated.

A third ethical challenge that must be discussed is the society and culture of fear and conformity that extensive surveillance creates. When individuals are subject to the thought that they are under surveillance and are being watched by the government for no reason, they live in a society of fear that they will be scrutinized and watched for simply saying something that may be politically opposed to the government's policies, or for being an active member in an Islamic community, or for traveling among different countries that are not diplomatically on good terms with the United States. Individuals who may fit the stereotypical profile of a terrorist are viewed with greater suspicion and judgment from their neighbors, as the public concern for safety has grown with each new

security measure and news of another attack around the world (Bloss, 2007, p. 223). Subjecting individuals to a life of judgment and suspicion goes against what this country stands for in its attempt to ensure freedoms and invitation for all individuals to live here; moreover, this dilemma links back with the previous section regarding racial and religious, among others, discriminations and stereotyping that cause certain individuals to feel unwelcome and unable to avoid judgment.

A fourth ethical concern is the honesty and transparency that must surround the surveillance program. While it is impossible for the various agencies and organizations to fully disclose all of the security measures that they have in place, as secrecy is the nature of their work, it is still important to determine whether or not they are intentionally lying to the public and to the authorities about the width of their surveillance and the level of intensity that individuals are subjected to. Accountability within the domestic surveillance environment is limited, as the organizational structure is uncertain and jurisdictional lines are blurred between agencies on all levels. Dahl (2011) highlighted this lack of organization and oversight when he wrote, “The problem is that Congressional oversight of intelligence matters is widely regarded as weak” and “Although most local fusion centers receive federal funds and receive operating guidelines from DHS and the Department of Justice, they are under state or local control and as such are not subject to any strong, centralized oversight” (p. 5). Because of this lack of clear accountability, the public are not able to be adequately protected from violations of their rights and can be easily taken advantage of by the legislators and agencies who seek to create an even greater surveillance system. For criminal justice professionals, whether law enforcement officers or federal employees, it is important to

consider this question of whether or not they believe it is acceptable to continue to push the boundaries of legality and simply expand on the surveillance of citizens because there is weak accountability who cannot deny their expansion.

A final area that is concerned more with legality and less on an ethical standard is the question of actions taken after identifying American citizens as terrorists. As they are American citizens and protected by the Constitution, what actions are allowed to be taken to stop them from plotting against other citizens or carrying out these attacks? The Constitution guarantees due process and the right to a trial, but some would argue that these individuals should be considered combatants in war and can be detained in military custody even though they are not specifically in the military (Senate RPC, 2013). Even though they are terrorists, their rights as American citizens to be treated fairly and present their case in a courtroom must still be considered and discussed; for criminal justice professionals, it presents a conflict between those who believe in upholding the Constitution no matter what and those who are under the impression that threats must be dealt with and those who engage in terrorist activities, no matter their citizenship, have given up any right to a trial in their attempts to hurt innocents.

Christianity and the Future of Surveillance

While these ethical concerns can be applied to a Christian in criminal justice, an examination of the possible future of domestic surveillance from a Christian worldview must also be explored. Although the future is by no means clear and certain events and individuals all can affect the direction that homeland security measures take, nevertheless it is important to discuss the possible future for America's domestic surveillance system and Christianity in order to create individuals who can clearly determine their principles

in this difficult environment. Christians who are entering this world of surveillance and secrecy must be aware of the difficult decisions that they must wrestle with regarding the ethical dilemmas previously discussed and others that come into conflict with their beliefs and worldview.

As criminal justice and the world of law enforcement has grown and the depravity of man has become ever clearer with the growth of technology, it is crucial that Christians in each generation rise to the occasion and is aware of the need of strong Christians who can see the evil that is present in the world and still cling to their hope of redemption and salvation in Christ. In His Word, God calls for justice and integrity from His people, such as in Amos 5:24 which says "But let justice roll down like waters, and righteousness like an ever-flowing stream" (ESV) and Micah 6:8, which states "He has told you, O man, what is good; and what does the Lord require of you but to do justice, and to love kindness, and to walk humbly with your God?" (ESV). Since Christians must be just and righteous, they must be critical thinkers and analyzers about the consequences of conscious violations of privacy while balancing the need to bring justice to those who seek to and do commit crimes against innocent citizens.

The Struggle of Good and Evil

Too often, the discussion of domestic surveillance is reduced to a simplistic choice between good and evil, no matter which side of the debate an individual is on. For those in favor of surveillance, additional security measures are the clear "good" and those who want to limit the power of the government to protect the citizens are "evil"; on the opposite end, those who want to protect the constitutional right to privacy are "good" and the government seeking to overstep its bounds is "evil" and must be resisted. Domestic

surveillance is much too broad and complex to simply be good or evil, and thus should be debated bearing the ethical concerns discussed previously. Christians in the law enforcement world and as citizens must raise their voices and join the debates surrounding counterterrorism and domestic surveillance, as they can be a part in influencing those in authority to limit the surveillance practices if they have taken a step too far.

For Christians in this field, a difficult decision arises when faced with the issue of authority. As each Christian may have a different view of what is moral and righteous, obeying the orders that those in authority pass down can become an ethical dilemma. For a Christian working in the NSA or another surveillance agency, the issue of violating citizens' privacy rights will arise, and thus causes a dilemma of whether or not to obey the authority figure that has ordered surveillance to be conducted. God calls for Christians to obey those placed in power above them, as Romans 13:1 says, "Let every person be subject to the governing authorities. For there is no authority except from God, and those that exist have been instituted by God" (ESV). While it is easy for anyone to obey those that they agree with and hold the same beliefs as them, it is much more difficult to obey those who do not share the same moral values. For a Christian who does not agree with the mass surveillance techniques and warrantless monitoring that the government conducts, it presents an ethical dilemma as they must decide whether or not to obey an individual who has been tasked with ensuring the safety of the nation and believe that infringing on privacy rights is a small price to pay in order to keep the nation's citizens alive and well.

The Future of Domestic Surveillance

As technology expands its influence and those who wish to generate harm to innocent people develop new avenues of attack, the United States must be constantly thinking about new ways to counter these threats and protect its citizens. Because of the vast scale of surveillance and numerous agencies and organizations involved, many scholars have recommended that a more centralized and better coordinated surveillance system and policies be enacted by the federal government to provide some oversight and foundation in order to more efficiently provide accountability and feedback to the American public (Carter, Deutch, & Zelikow, 1998; Martin, 2004; Perl, 2001; Rosenbach, 2008). Better coordination and communication by federal agencies with one another, federal agencies with state and local agencies, and with the private sector must be a fundamental and foundational goal for the government, as this can help eliminate unnecessary data acquisition and streamline the process of finding terrorists or potential terrorists.

Clear guidelines and goals for intelligence gathering must also be established and set forth to prevent innocent, unsuspecting citizens from being monitored. Establishing a strategy and obtaining quality intelligence must be a key goal for the intelligence community, in order to best share information with other agencies and produce the most information on potential targets and threats. Rosenbach (2008) stated,

> The intelligence community needs to focus on its analytic efforts on strategic assessments of terrorist leadership and operational plans, ensuring the quality of terrorist watch lists and providing operational personnel with the granular 'tactical' intelligence that they need to eliminate or capture terrorists. (p. 140)

Proper analysis of intelligence and data that come in from surveillance and monitoring must be utilized to create an all-encompassing report of the most dangerous threats and integrate all available information in order for agencies and law enforcement to be best prepared for the danger that they present. This high-quality and plentiful amount of intelligence that has been analyzed should be a goal for future organizations to strive towards, as this can ensure a more coordinated and structured security system that has the proper channels of communication open to work together to stop all threats.

The judicial system is also an important factor when discussing the future of domestic surveillance, as they must be able to support FISA and fight back against any surveillance or investigation that has not properly followed the existing legislation or has not provided proper evidence of misconduct. Henderson (2002), when he discussed the judicial system's potential to uphold FISA, said, "the courts could act as an independent check on executive authority" (p. 208), and cited specifically that they should be given the ability to exclude any evidence found in an investigation in which national security was not a significant purpose, as well as be able to have the government "check-in" periodically to assess the necessity for roving surveillance (p. 209). Enabling the judiciary with the ability to limit governmental overreach and entrusting them with the oversight and interpretation of policies and legislation enacted is crucial for the future and balance of domestic surveillance, as privacy versus security will continue to dictate further security measures.

While the future of surveillance can be put to good use and reformed so as to better detect threats to the safety of the nation, there is also great potential for even more harm and reduction of privacy rights. Many scholars have noted the danger that is

presented when personal liberties are brushed aside in the name of security. Haggerty and Gazso (2005) wrote, "…we are undeniably in the process of trading some freedoms for the promise of greater security, and as such must remain vigilant to ensure that we might not have already skewed the balance too far in one direction" (p. 185). Lewis (2005) wrote, "The most significant domestic issue raised by the pivotal event on September 11, 2001, and its aftermath is the extent to which civil liberties are to be curtailed to fulfill the government's responsibility to ensure domestic tranquility" (p. 27). Henderson (2002) said, "…the executive's authority to conduct electronic surveillance cannot be restricted as Congress intended unless the judiciary remains cognizant of the oversight responsibilities with which it has been entrusted" (p. 209). The recognition of the potential for greater abuse and realization that greater awareness must be made is a step towards restoring the balance of security and privacy, and should continue for future scholars and criminal justice professionals.

Conclusion

As this thesis has sought to show, domestic surveillance is a complex and ever-changing topic within the criminal justice world, and must be constantly discussed and researched in order to continuously evaluate the difficult balance between privacy and security. The U.S. government has expanded its power and created a vast system of surveillance in order to monitor citizens and promote their safety, but has also struggled with containing its practices within the bounds of the Constitution. The ethical dilemmas of such secretive and warrantless surveillance will continue to grow as technology advances and new issues with surveillance arise, which must be further researched and discussed as they develop. The future of domestic surveillance must be approached with

caution and a willingness to bring about reform, so that intelligence agencies can limit their data gathering and share the pertinent information with one another to effectively fight against terrorism.

References

American Civil Liberties Union. (n.d.). Surveillance under the usa/patriot act. Retrieved from https://www.aclu.org/other/surveillance-under-usapatriot-act

American Civil Liberties Union. (n.d.) About the aclu. Retrieved from https://www.aclu.org/about-aclu

Bernal, P. (2016). Data gathering, surveillance, and human rights: Recasting the debate. *Journal of Cyber Policy, 1*(2), 243-264. doi: 10.1080/23738871.2016.1228990

Black, D. (2004). The geometry of terrorism. *Sociological Theory, 22*(1), 14-25. Retrieved from https://doi.org/10.1111/j.1467-9558.2004.00201.x

Bloss, W. (2007). Escalating u.s. police surveillance after 9/11: An examination of causes and effects. *Surveillance and Society, 4*(3), 208-228. Retrieved from https://panoptykon.org/sites/default/files/3448-5760-2-pb.pdf

Carpenter v. United States, 585 US _ (2018)

Carter, A., Deutch, J., & Zelikow, P. (1998). Catastrophic terrorism: Tackling the new danger. *Foreign Affairs, 77*(6), 80-94. Retrieved from https://www.jstor.org/stable/20049132

Dahl, E. (2011). Domestic intelligence today: More security but less liberty? *Homeland Security Affairs, 7,* 1-9. Retrieved from https://www.hsaj.org/articles/67

Deflem, M., & McDonough, S. (2015). The fear of counterterrorism: Surveillance and civil liberties since 9/11. *Global Society, 52,* 70-79. doi: 10.1007/s12115-014-9855-1

Giroux, H.A. (2015). Totalitarian paranoia in the post-orwellian surveillance state. *Cultural Studies, 29*(2), 108-142. doi: 10.1080/09502386.2014.917118

Goodman, M. (2015). *Future crime.* New York, NY: Doubleday.

Haggerty, K.D., & Gazso, A. (2005). Seeing beyond the ruins: Surveillance as a response to terrorist threats. *The Canadian Journal of Sociology, 30*(2), 169-187. Retrieved from https://www.jstor.org/stable/4146129

Henderson, N.C. (2002). The patriot act's impact on the government's ability to conduct electronic surveillance of ongoing domestic communications. *Duke Law Journal, 52,* 179-209. Retrieved from https://scholarship.law.duke.edu/dlj/vol52/iss1/3/

Katz v. United States, 389 US 347 (1967)

Laidey, N.M. (2015). Privacy versus national security: Where do we draw the line? *International Scholarly and Scientific Research and Innovation, 9*(6), 2235-2238. doi.org/10.5281/zenodo.1110387

Landau, S. (2013). Making sense from snowden: What's significant in the nsa surveillance revelations. *IEEE Security and Privacy, 11*(4), 54-63. doi: 10.1109/MSP.2013.90

Lewis, C.W. (2005). The clash between liberty and security in the u.s. response to terror. *Public Administration Review, 65*(1), 18-30. Retrived from https://www.jstor.org/stable/3542578

Martin, K. (2004). Domestic intelligence and civil liberties. *SAIS Review, 24*(1), 7-21. Retrieved from https://pdfs.semanticscholar.org/9bb0/1e307b4a66c842c5bf37935746fa01a2d5a9.pdf

Monahan, T. (2010). The future of security? Surveillance operations at homeland security fusion centers. *Social Justice, 37*(2/3), 84-98. Retrieved from

https://www.jstor.org/stable/41336984

Orwell, G. (1949). *1984.* London, UK: Secker and Warburg.

Perl, R. F. (2001). *Terrorism, the future, and u.s. foreign policy.* (Library of Congress Washington, D.C., Congressional Research Service), 1-18. Accession Number: ADA481133. Retrieved from https://apps.dtic.mil/docs/citations/ADA481133

Powell, K.A. (2011). Framing islam: An analysis of u.s. media coverage of terrorism since 9/11. *Communication Studies, 62*(1), 90-112. doi:10.1080/10510974.2011.533599

Rokos, B. (2016, June 12). Orlando mass shooting: Similarities between the Orlando, San Bernardino attacks are jarring to read. *The Press Enterprise.* Retrieved from https://www.pe.com/

Rosenbach, E. (2008). The incisive fight: Recommendations for improving counterterrorism intelligence. *The Annals of the American Academy of Political and Social Science, 618,* 133-147. Retrieved from https://www.jstor.org/stable/40375780

Senate Republican Policy Committee. (2013). *U.S. citizen terrorists.* Policy Papers. Retrieved from https://www.rpc.senate.gov/policy-papers/us-citizen-terrorists

U.S. Senate. (n.d.). Senate select committee to study governmental operations with respect to intelligence activities. Retrieved from https://www.senate.gov/index.htm

Yoo, J. (2007). The terrorist surveillance program and the constitution. *George Mason Law Review, 14*(3), 565-604. Retrieved from https://scholarship.law.berkeley.edu/facpubs/168/

Zwerman, G. (1989). Domestic counterterrorism: U.S. government responses to political violence on the left in the reagan era. *Social Justice, 16*(2), 31-63. Retrieved from https://www.jstor.org/stable/29766463