# CHOOSING SECURITY OVER FREEDOM: THE INTERSECTION OF TECHNOLOGY AND PRIVACY IN A POST-9/11 WORLD

By

MARIAH HOPE LATIMER

_____

A Thesis Submitted to The Honors College

In Partial Fulfillment of the Bachelors Degree
With Honors In

Criminal Justice

THE UNIVERSITY OF ARIZONA

MAY 2018

Approved by:

_____

Professor Kristine Huskey
James E. Rogers College of Law

*The September 11, 2001 terror attacks had a far-reaching, global impact. Within the United States, lawmakers rapidly sought to address the aftermath by passing strong anti-terrorism policies. Other nations followed suit. At first, few people dared to question the implications of these policies. Nearly two decades later, technological advancements and a heightened concern over governmental restrictions on liberty are forcing policymakers to reexamine the legality of governmental invasions of privacy in the name of national security. This Paper examines the reach of U.S. anti-terrorism policies and their impact on individual privacy, the realities of similar policies in the United Kingdom, and the effectiveness of these policies in protecting national security. Additionally, this Paper explores the tension between privacy and security interests, both at home and abroad.*

## INTRODUCTION

One of the purposes of an organized government is to ensure the safety and security of its citizens. This guarantee preserves the nation as a whole, as well as the quality of life a country's citizens expect. Providing for the security of a government's citizens makes sense economically, socially, and politically. Like all government endeavors, however, security comes at a cost. Effective solutions can require substantial fiscal investments. Even more, many modern security solutions necessarily invade privacy as a cost of providing safety.

Public opinion in the United States regarding this trade-off has fluctuated greatly over time, largely mimicking the immediate concerns of the country as opposed to sustainable long-term goals. Soon after the September 11, 2001, terrorist attacks, the U.S. public demanded legislative reform and called for accountability. September 11 not only impacted American policy, however, as a multitude of countries implemented policies that mirrored the United States' post-9/11 actions. This Paper compares the United States' and the United Kingdom's policies in this arena, with particular emphasis on England's policymaking approach. This comparison is particularly informative due to the strong similarities in language and culture, as well as each country's concern for national security.

This Paper proceeds in three parts. In Part I, this Paper explores what the terms *privacy* and *security* mean as it pertains to anti-terrorism and national security goals and the role of advanced technology in pursuing these goals. In Part II, this Paper addresses the arguments for and against the government's increasing use of such technology in the United States in

the name of national security and at the expense of individual privacy. Part II also compares the social and legislative climate immediately after September 11 with the social and legislative climate in the context of Edward Snowden and the 2013 National Security Agency revelations. Finally, Part III compares the efficacy of recent restrictive security policies and pro-privacy reformative actions taking place in the United States to the lack of similar policymaking endeavors in the United Kingdom, which reveals these nations' different priorities and power structures. This Paper then concludes that the United States has taken appropriate steps towards rebalancing the need for both privacy and security, while the United Kingdom has continued to adhere to policies that largely sacrifice individual privacy rights for the advancement of national security without significantly preventing ongoing terrorist activity within its own borders.

## I. THE STRUGGLE TO DEFINE PRIVACY AND SECURITY IN A POST-9/11 CLIMATE

Privacy is something to be valued by the members of any society. This is particularly true, however, in a democratic society like the United States, a country dedicated to upholding certain freedoms and preserving liberty. But individual privacy is at odds with increased security, and the average American yearns for both, which leaves policymakers the difficult task of balancing these opposing interests.

To further complicate the matter, defining privacy and establishing the scope of privacy rights is a complicated endeavor, especially in the United States. This is, in part, due to the United States Constitution, which guides the formation and assessment of government action. Unfortunately, however, the Constitution provides little guidance when it comes to privacy issues. As noted by Amitai Etzioni, "the US Constitution does not so much as even mention privacy. Not once. Privacy is a constitutional right fashioned only in the mid-1960's; that is, it is of very recent vintage."[1]

Etzioni is referring to a pair of Supreme Court cases that established the concept of legal privacy, as we know it today: *Griswold v. Connecticut*[2] and *Roe v. Wade*.[3] *Griswold* established an individual's right to contraception, while *Roe* established an individual's right to an abortion. Admittedly, these

[1] Amitai Etzioni, *The Limits of Privacy*, 2000

[2] *Griswold v. Connecticut* (1965), The Supreme Court ruled that states cannot ban the right to use contraceptives and that individuals have a constitutional right to privacy in this matter, implied by the Bill of Rights.

[3] *Roe v. Wade* (1971) The Supreme Court ruled that a Texas law prohibiting abortion except in cases where a woman's life was in danger was unconstitutional, establishing a personal right to bodily privacy.

topics are not what normally come to mind when discussing privacy rights, at least not in the context of national security. Still, *Griswold* and *Roe* were each instrumental in forging modern notions of individual privacy. *Griswold* declared that couples have the right to use contraception without regulation from the government, essentially creating a sense of privacy surrounding the intimate lives of U.S. citizens. Additionally, the ruling in *Roe* effectively declared that the U.S. government should not play a role in determining what a woman is legally allowed to do with her own body and that women should have a choice when it comes to aborting a fetus. While there are still some government regulations that limit a woman's personal privacy in regards to abortion (the illegality of abortions in the third trimester, or a minor needing parental consent to receive an abortion, for example) *Roe* set the precedent that a woman has the right to make her own reproductive choices without undue interference from the government.

While Supreme Court cases such as *Griswold* and *Roe* established a legal precedent for specific privacies, the Fourth Amendment provides the most wide-ranging and powerful foundation for defining the legal bounds of privacy in the United States. Upon examining the language of the Fourth Amendment, however, it seems to lack the strength of other provisions in the Constitution, such as the First Amendment's protections of religion, speech, and the freedom of assembly. Notably, the Fourth Amendment does not outlaw the government's right to conduct searches and seizures. Rather, it imposes limits and prohibits only unreasonable searches and seizures. In fact, the Supreme Court has "long held that 'the touchstone of the Fourth Amendment is reasonableness.'"

In other words, the Fourth Amendment does not provide an inalienable right to privacy, but merely restricts the government's invasions of individual privacy to only those that are "reasonable." But reasonableness can be difficult to define. Etzioni addresses the consequences of the reasonableness standard:

> Privacy advocates often argue that our rights have been violated when new security measures or anti-crime measures are introduced – for instance, cameras in public spaces. However, if these new measures are reasonable, then no one's right has been violated – no privacy has been lost or violated – in the legal sense. People cannot give up what they never had and they never had a legal right against all searches.[4]

Etzioni's point is an interesting one; he seems to believe that citizens cannot be deprived of a right that they never had to begin with. This seems to make sense at first glance, but a closer examination questions whether the reasonableness standard defines the scope of an individual's right to privacy or whether it defines the government's ability to invade a right that exists

[4] Amitai Etzioni, *The Limits of Privacy*, 2000

independently of the Fourth Amendment. This skeptical approach to legal protections of individual privacy is an example of but one approach to addressing the tension between individual privacy and national security. Etzioni's perspective, that law defines the scope of an individual's right to privacy, is on the opposite side of the same coin.

When it comes to the debate regarding sacrificing individual privacy in the context of preserving national security, there is a disagreement of opinion in defining the term 'privacy' in the first place. While some regard privacy to be a fundamental right that must exist separately from the institution of government, other feel as though privacy is a right that exists as a legal right, granted only insofar as a government allows it.

The United States has a history rooted in a desire to protect the concept of freedom for all of its citizens. Desiring freedom from an oppressive British government motivated the founding fathers to establish a government that would highlight personal freedoms, and as such, the Bill of Rights was created as the first ten amendments to the Constitution. Although a right to privacy was never explicitly written in the Bill of Rights, the importance of personal freedoms was certainly emphasized in the founding of the United States. Taking this into account, it is understandable why some view a right to privacy as being an intrinsic value that must be guaranteed by the U.S. government.

In order to approach a complicated debate, it is crucial to pick apart the components of the issue and boil them down to their simplest forms. Therefore, for the purposes of this Paper and for the sake of comparing the United States and the United Kingdom, *privacy* will be defined here on out as *acting without the interference of government*. Interference can be anything that complicates or prevents said person from carrying out an action, and it can also include *unwilling* observation of activities. For example, going through security at an airport would be considered an infringement upon privacy, as the individual's choice of choosing air travel is being complicated by the regulations of a certain government. Additionally, surveillance of a person's home or whereabouts is in violation of their personal privacy, but a person's willful interaction with such observation is not, such as entering a store that openly employs the use of security cameras. Privacy is something that a person may choose to relinquish.

However, it is important to note that infringement upon privacy is not necessarily a negative concept. In the airport security example, a person's privacy is being compromised, but this does not mean that it is unreasonably so. There is a certain amount of privacy that must be sacrificed in the realities of a modern world, the issue is in determining how much, and at what cost. This is where the idea of reasonableness becomes

important to consider.

To further complicate matters, defining what is reasonable in society is a concept that changes as social conditions change. For example, what is widely considered reasonable immediately after an event like September 11 is drastically different from what society considers reasonable during a time of stability and peace. Laws change much slower than society evolves, however, and the policies that were implemented in the wake of September 11 were hasty, to say the least.

This seems to be true of wartime policy decisions generally. Take, for example, the U.S. Supreme Court's opinion in *Korematsu v. United States*. In that case, which was decided in the hysteria surrounding World War II, the Supreme Court held that the U.S. military could lawfully confine persons of Japanese descent in concentration camps. The fear was that individuals of Japanese descent, even Japanese Americans, may be foreign operatives working in the U.S. to further Japanese military interests. In today's racial climate, this type of large-scale, race-based discrimination would almost undoubtedly be unacceptable. But *Korematsu*, which was decided over 70 years ago and in a radically different social climate, has not been overruled. This poignant example illustrates how hasty but permanent policy decisions can persist for decades, long after the concerns that led to the policy have faded away.

The United States government wields a vast amount of power, even more so in a technologically advanced era. Theoretically, the power is meant to come from the bottom up; in a democracy, the voters dictate who is elected and how much power representatives should bear. After a catastrophic event like 9/11, however, the government is able to act in extreme ways without the interference of regular checks and balances. National security became the prime concern after 9/11, and most of the population was supportive of doing whatever necessary in the days, weeks, months, even years after the attacks.

As with any government, even a democracy, power comes with the danger of corruption. This is a concept that Adam D. Moore discusses in depth. Moore notes historical examples of the misuse of power, including *Korematsu*, and argues that, "[i]n cases where there is a lack of accountability provisions and independent oversight, governments may pose the greater security risk."[5] In short, government has the potential to provide for and destroy both security and individual privacy.

In the case of *Korematsu*, the U.S. government sacrificed the safety of its own Japanese American citizens for fear of a threat that was only perceived to be imminent. The issue of defining *security,* then, is more

[5] Adam D. Moore, *Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability*, April 2011

complicated than proactively disarming militaristic threats. The government must ultimately seek to protect and enhance the well-being of its citizens; when it oversteps those bounds, the government only succeeds in doing the exact opposite. For the purposes of this Paper, *security* will be defined as *the preservation of safety and comfort, from both real and perceived threats, provided by a government to its citizens*. This definition of security is multifaceted. It is crucial not only that a government is able to physically protect its citizenry, but that it is also able to provide a stable environment free from the fear or belief of a threat.

From this perspective, it is more clear why the government chose to intern Japanese Americans during World War II. Although it was a very poor policy decision in retrospect, the U.S. government was attempting to address a perceived threat of attack by the Japanese in order to further provide for the security of its citizens. Unfortunately, in an effort to be proactive, the government succeeded only in violating the human rights of many.

In present times, the U.S. government would undoubtedly handle the same situation much differently, but some would argue not much better in terms of violating personal privacy. Speculation as to how the government might have handled the attack on Pearl Harbor in the present day need not go much further than examining the reaction to 9/11. Though different in many respects, the two events both posed an immediate, major national security concern for leaders of the time. Though the idea of internment camps was not revisited in 2001, a shift in attitude towards persons of Middle Eastern descent as well as bulk data collection and surveillance all came to fruition. Something as widespread and invasive as bulk data collection was not possible during World War II, but technology has evolved extensively. Simply put, modern advances in technology have the capability to enable the government to better protect its citizens, but it also has the power to violate the citizens' privacy beyond benefit.

In the pursuit of national security, there is a widely held conception among intelligence analysts that technology theoretically has the potential to proactively eliminate all threats of terrorism. That is, in a world where the government has access to unlimited amounts of raw intelligence, the concern for security would only be a question of utilizing that intelligence in a way that would address threats before they occur. Knowledge serves as a form of militaristic defense in this way, and this notion has led the U.S. government to use technology in an effort to collect massive amounts of raw data on not only suspected terrorists, but also its own citizens. Moore argues that "an indication of power is the ability to forcibly demand access

to information about others while keeping one's own information secret."[6] The issue with government power is not that it is present, but that power combined with a lack of transparency creates a dangerous environment.

It is important to note, however, that government use of technology does not always lead to an infringement upon individual privacy; in many cases, technology has been used by the government to ensure that individual privacy is protected against industrial espionage, information warfare, terrorism, and unwarranted invasions into private domains, to name just a few examples.[7] Under the right circumstances, technology plays an important role in the advancement of national security interests.

Modern day terrorism and crime are often most dangerous on the technological front, with foreign entities increasingly turning to cyber strategies. The terms *cybercrime* and *cyberterrorism* represent areas of national security that are relatively new, and modern-day legislation has not been able to keep up with technological changes as fast as they've occurred. This has partially contributed to the implementation of policies in the U.S. that may or may not be constitutional; problematically, the oversight of the implementation of such policies was virtually nonexistent in the aftermath of September 11. Specifics regarding the capabilities of technology in both ensuring national security and invading personal privacy will be discussed in Part II of this Paper.

## II. Positive and Negative Impacts of Technological Advancements on Security and Privacy: Edward Snowden, the NSA, and Terrorism

The legislative response to the events of 9/11 occurred rapidly. On October 26th, 2001, President George Bush signed the USA Patriot Act[8] after the final version of the bill made its way through the House of Representatives and the Senate with overwhelming support.[9] At the time, there was confusion regarding how exactly the USA Patriot Act would affect the country going forward. Many politicians and laypersons were unclear about what the Act would entail; even today, there seem to be widespread misconceptions about the true impact the Act exerted.

---

[6] Adam D. Moore, *Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability*, April 2011

[7] Adam D. Moore, *Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability*, April 2011

[8] *See* Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, § 224, 115 Stat. 272, 295

[9] The House of Representatives approved the final bill by a vote of 356 to 66, and one day later, the Senate approved the final bill by a vote of 98 to 1. President Bush signed the bill into law the next day.

At its core, the Patriot Act modified existing laws in order to bring legislation up to speed with the technology of the time. Previous laws regarding surveillance were enacted before the Internet became a mainstream form of communication. Namely, the Foreign Intelligence Surveillance Act (FISA)[10] was the primary law modified by the Patriot Act. Contrary to popular belief, the Patriot Act merely strengthened existing governmental powers as opposed to creating entirely new ones.

On the surface, this fact seems to weaken the argument that the Patriot Act stands for an unreasonable intrusion into personal privacy. However, as scholar Daniel Solove puts it, "Privacy is often threatened not by a single egregious act but by the slow accretion of a series of relatively minor acts."[11] From this perspective, modifications implemented through the Patriot Act may be minor in comparison to the original powers granted by FISA, but this does not mean that such modifications are insignificant in the overarching struggle to preserve privacy. Therefore, one must dig deeper into the ramifications, or lack thereof, of the Patriot Act in order to identify whether or not the act constitutes an unreasonable erosion of privacy.

Although the Patriot Act is commonly thought of as being a singular event that granted the U.S. government sweeping new powers, it is difficult to support this notion due to the complexity of the Act itself. The Act is an enormous collection of amendments to federal law and addresses much more than just Internet surveillance.[12] Being so large and complex makes the Act difficult to characterize, especially with such broad generalizations. To analyze the true effects of the Act would mean understanding the intricacies involved with issues "ranging from immigration to money laundering."[13]

The popular attitude towards the Patriot Act has evolved over time, and in the immediate years following 9/11, the Act was viewed as a positive government response taken in order to preserve the future safety of the United States. However, in more recent times, the American population has grown increasingly wary of government powers that may infringe upon personal liberties. According to the Pew Research Center, as of October 25, 2001, just one day before President George Bush signed the Patriot Act, public trust in government was polled at 54%.[14] For context, the same poll

---

[10] *See* The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, 1861-62, 1871.

[11] Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, February 2008

[12] Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 2002

[13] Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 2002

[14] Pew Research Center, *Public Trust in Government,* May 2017

hadn't reached as high as 54% since December of 1970, during the Nixon administration. This percentage was measured as the percentage of people who trust the government in Washington 'always or most of the time'. Since this data point in 2001, public trust has shown to be in decline. The poll statistics, which have been measured since December of 1958, certainly show variation over time. Notably, however, in May 2013, this number had declined to a staggering low of 20%.[15] The Pew Research Center shows that a percentage this low hadn't occurred since 1994. Table 1 has been included to illustrate this data.

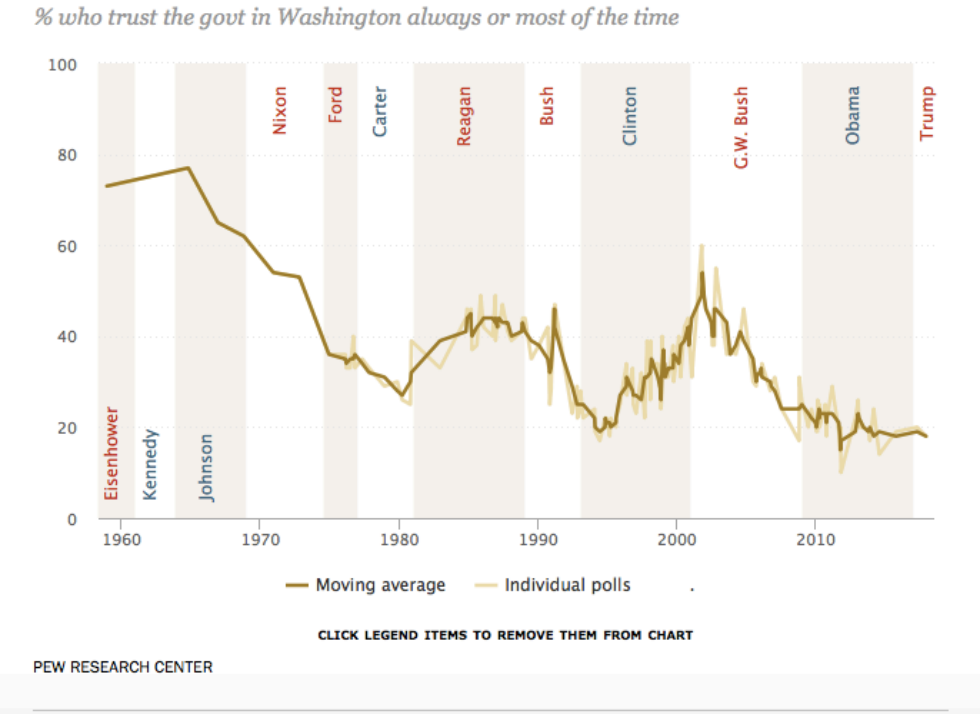


Table 1: Pew Research Center, *Public Trust in Government,* May 2017

The public's trust in government undoubtedly reflects the social and cultural environment of the time; citizens expect their government to be able to handle problems that arise and to do so fairly and ideally, with transparency. While there is a certain level of secrecy that must be protected in the pursuit of national security, the American public has come to expect the government to perform its core functions in a way that allows democracy to reign in any questionable behavior. The problem, then, is in the fact that there is not enough transparency for the public to make

[15] Pew Research Center, *Public Trust in Government,* May 2017

informed decisions within an organized democracy to dictate the actions of their government.

In May 2013, the point at which public trust in government fell to a measly 20%, something occurred that changed the way that the American public will forever view the intersection of government affairs and technology. At this time, Edward Snowden orchestrated the release of thousands of classified government documents. While perhaps this fall in government trust can be attributed to a variety of intermingling factors, the impact of Snowden's actions cannot be overlooked. By exposing the extent of the secretive technological surveillance being utilized by the U.S. government, Snowden further cemented the idea that the government lacks the necessary transparency to uphold the ideals of a fair democracy. In essence, Snowden exposed the extent to which the NSA, and by extension the United States, uses technology to gather and store a massive amount of private information.

Revealed by the classified documents, it came to light that the NSA was utilizing wiretapping and the collection of metadata from private companies and Internet communications. One of the tools used to execute this is PRISM, a program used by the NSA to collect technological surveillance.[16] While the U.S. government has participated in wiretapping for decades, according to Susan Landau, "Although there might have been surveillance abuses post- FISA, those that have come to light were relatively small in scale until after 11 September 2001."[17] In the wake of 9/11, the National Security Agency (NSA) identified large-scale data mining to be the best offensive weapon at the United States' disposal. Particularly, Internet communications offered a wealth of untapped information regarding potential terrorist activities; at the time, terrorist organizations were primarily using U.S. webmail accounts to communicate.[18] While the NSA could have pursued an emergency FISA order in order to obtain this metadata through the proper legal channels, the political environment immediately after 9/11 was fraught with uncertainty and a desire to act quickly in the face of impending danger.

One issue regarding the actions taken by the NSA after 9/11 is that the law has not been able to keep up with certain advancements in technology. Part of the information collected by the NSA, and then eventually exposed by Snowden, involved the collection of cell phone metadata. Although the

---

[16] Lavanya Rathnam, *PRISM, Snowden and Government Surveillance: 6 Things You Need To Know,* April 2017

[17] Susan Landau, *Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations*, July/August 2013

[18] Susan Landau, *Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations*, July/August 2013

NSA was collecting metadata as opposed to content, the amount of information that can be obtained about a person through metadata alone is perhaps more impactful than most American citizens may realize. The difference between content and metadata is a noteworthy distinction: whereas content reveals the exact communication exchanged between multiple parties, metadata is concerned only with information about such communication. For example, from cell phone metadata, one can potentially determine the location of the user at any given time while using the cell phone, the timing of said communications, and with whom a person is communicating. Combined, these insights into an individual's life have the capability to tell law enforcement an extensive amount about a person's private exchanges.

The collection of metadata, or even the content of specific communications, is not alone considered to be an invasion of privacy under the Constitution. Rather, just as with any search and seizure, there are standards to regulate when and how the collection of private information by the government is legal. Problematically, in the wake of terrorism, the U.S. government chose to respond by selectively ignoring the usual channels of obtaining a FISA warrant. A government that chooses to ignore its own laws when it is convenient to do so is far from exemplifying democracy, and this is precisely what occurred when the NSA began to seize massive amounts of data in the name of national security.

Aside from the questionable decision to pursue bulk data collection outside of the proper legal channels, the question of whether or not the NSA should be able to conduct surveillance on such a grand scale is the true heart of the ongoing debate between privacy interests and national security. Snowden believed that by releasing classified documents, he was standing up for personal liberties; in contrast, Senate Select Committee of Intelligence Chair Dianne Feinstein called Snowden's actions "treasonous", and Feinstein was not alone in this conviction.[19] In fact, the response to Snowden's actions has been mixed across the board. Feinstein, a Democratic Senator from California and Current Republican President Donald J. Trump both were quick to label Snowden as guilty of treason.[20]

Others applaud Snowden's decision to release the documents and cite the surveillance as an abuse of power, but it cannot be denied that Snowden knowingly exposed information that had the potential to threaten United States security interests. Working as a contractor for the NSA, Snowden was not amongst those whom collected, analyzed, or acted upon intelligence and lacked the specialized knowledge to judge the potential

[19] Jeremy Herb, *NSA leak is treason, says Feinstein*, June 2013

[20] Cheryl K. Chumley, *Donald Trump on Edward Snowden: Kill the 'traitor'*, July 2013

implications of his actions. Additionally, it is somewhat challenging for the public to measure the subsequent consequences of bulk data collection, as it serves as a tool for proactive antiterrorism. In exchange for this proactivity, the public unknowingly provided personal data to be examined by the NSA.

Both the costs and benefits that technology provides to antiterrorism efforts should be taken into consideration in order to analyze whether or not a sacrifice of privacy is warranted. This question is not one with a clear-cut answer, and more or less shaped by individual values and biases, but such an analysis is beneficial regardless. In a democracy like the United States, it is vital for citizens to be able to call into question the actions of the governing body and to continually assess the Constitutionality of various policies. Therefore, exploring the realistic extent to which technology, such as wiretaps, government surveillance programs, security cameras, or any number of electronic devices, helps or harms individual privacy is crucial.

Using bulk data collection as an example, the tangible harm that comes from government access to such a vast amount of private information is challenging to measure. The greatest threat that comes from bulk data collection seems to largely be symbolic; the fear does not come mainly from the possession of the information itself, although this is a possibility as well, but from the idea that the government can seize such information at will.

The most widely cited argument against this fear is the idea that if an individual has nothing to hide, then they should not be affected by or opposed to government surveillance. Within this mindset, even the simple act of resistance may be construed as suspicious or unpatriotic. Adam Moore argues that this perspective is flawed and far too simplistic. In support, Moore draws on examples that include sexuality, religious beliefs, and political party affiliations in order to show that information, aside from criminal activity, can be sensitive to the person under surveillance.[21] Although the NSA is largely unconcerned with the personal lives of non-terrorists, it remains that bulk data collection has the potential to expose these types of particulars of which the individual would rather not share. Specifics as to why someone may or may not wish to share the intimate details of their lives with the NSA, or any other private or government agency is not of importance. Rather, what matters is that a person has the ability to choose what details he or she wants to share publicly; this is at the core of what it means to truly have privacy, and by extension, freedom.

Admittedly, the cost associated with this again proves to be of a symbolic nature, however; prior to the Snowden leaks, American citizens were not aware that their data was being harvested. Theoretically, the

[21] Adam D. Moore, *Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability*, April 2011

precise details of a person's sexual, ideological, or political affiliations were of no interest except when paired with evidence of ties to terrorism; the NSA, nor any other government agency, has enough resources to collect, process, and analyze the vast amount of raw data recovered from wiretapping. Ultimately, Moore does well in accounting for the individual reasons a person might be less inclined to voluntary give up personal information, but it is problematic to compare criminal activity to sexual orientation or political affiliations. One may wish to keep the latter two things private for various personal reasons, but when weighing the benefits of a secure nation next to a desire to conceal noncriminal personal facts from a government agency like the NSA, it becomes increasingly difficult to justify trading proactive national security measures for a symbolic comfort. Although the concept of 'national security' is somewhat comprised of symbolic values as well, there is also a degree of tangible benefit that accompanies a secure country. A smaller number of fatalities of American citizens both at home and abroad as well as fewer terrorist attacks globally are both measurable benefits to a proactive approach of using technology for antiterrorism purposes.

In addition, the advantages of the increased use of technology to battle terrorism go beyond the obvious of helping to thwart physical acts of harm. Much like having personal privacy, national security offers many symbolic effects. After 9/11, Americans were preoccupied with fear. National security became the President's first priority as well as the public's. Citizens wanted to know how the attacks were allowed to occur in the first place and what would be done to ensure that nothing of the sort would continue to happen. In response, the U.S. government undertook the daunting task of restoring a sense of ease to its people. In President Bush's first address to the country after the attacks, he said the following:

> These acts of mass murder were intended to frighten our nation into chaos and retreat. But they have failed. Our country is strong…Terrorist attacks can shake the foundations of our biggest buildings, but they cannot touch the foundation of America…Immediately following the first attack, I implemented our government's emergency response plans. Our military is powerful, and it's prepared.[22]

The wording of President Bush's 9/11 Address to the Nation was undoubtedly chosen with great care. In the aftermath of such a disastrous event, it was crucial for the President to reassure Americans that their country was strong and powerful. The President goes on to say that the American military would prevail, his words attempting to serve as comfort in the face of uncertainty. In the days after the attacks, parents chose to keep their children home from school, others were afraid to go to work, and many sat glued to television sets, watching and re-watching news coverage.

---

[22] President George W. Bush, *9/11 Address to the Nation*, September 2001

Ultimately, words of assurance are not enough to convince a nation that they are safe from threat. Rather, trust and sense of safety are hard earned.

It is ultimately challenging for a country to operate under the shadow of fear, and a strong sense of national security helps to ease the tension of uncertainty. An example of this could be as simple as security cameras in airports, or the knowledge that the NSA has the technology to actively monitor considerable threats of terrorism.

In conclusion, both privacy and national security interests are influenced by the government's access to advancing technology in symbolic ways, for better or worse. In attempting to analyze the positive and negative consequences that technology has had in each area, it is important to recognize that the value assigned to each consequence may vary according to personal values and that the two areas are too closely intertwined for such considerations to be clear cut issues. As Moore explains, "It is false to claim that in every case, more privacy means less security or more security entails less privacy."[23] Aside from symbolic consequences, however, it remains that in an effort to strengthen national security, the government aims to preserve the physical well being of its citizens, a consequence that can be more easily measured. While it may not be possible to accurately measure the number of lives saved or incidences avoided since 9/11 due to increased security measures, a lack of another set of catastrophic events the size of 9/11 may be observed as a distinct victory.

When basic needs are not met, such as food, water, or a sense of security, there is little room to prioritize symbolic values. It is possible to assess the relative comfort of the American population when it comes to security by looking at which areas of policy are being most vehemently advocated for. With privacy rights at the forefront of national concern, one may deduce that Americans feel safe enough from the possibility of another large-scale terrorist attack to now prioritize their intangible needs.

## III. The Efficacy of Pro-Security Policies, Recent Pro-Privacy Reforms in the United States, and Why the United Kingdom Hasn't Followed Suit

In many ways, the United Kingdom, specifically England, is similar to the United States. Sharing a primary language as well as many cultural and social practices, the two regions offer an opportunity for comparison when it comes to the efficacy of national security policies and the institution of pro-privacy laws. Terrorism is not a distinctly American issue by any means, and the United Kingdom has faced increased terrorist activities in

[23] Adam D. Moore, *Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability*, April 2011

recent years amidst the rise of the Islamic State of Syria and Iraq, or ISIS.

In May 2017, a terror attack in Manchester, England claimed the lives of 22 concertgoers. The perpetrator was a suicide bomber whose motivations were later revealed to be linked to ISIS; the Islamic State publicly claimed responsibility for the attack and praised the bombing.[24] Only a month later, in June 2017, another act of terrorism occurred in London when three assailants drove a car into pedestrians, followed but a series of stabbings. In total, seven victims perished and forty-eight others were injured in the attack for which ISIS would later boast responsibility.[25] Separately, these targeted acts of violence have taken place on a smaller scale than the infamous events of 9/11, but more or less have similar effects. The frequent nature of the attacks combined with varying methods of violence strategically perpetrated by ISIS is successful in that it inspires terror and uncertainty in an entire population.

Despite the fact that terrorist organizations have evolved and adapted to new security measures by using smaller, targeted attacks as opposed to fewer large-scale attacks, the core problem remains the same. Governments must take steps to protect its citizenry, regardless of what form such danger presents itself. In response to the last few decades of terror, first with Al-Qaeda and presently with ISIS and other smaller organizations, the United Kingdom has chosen to exercise its ability to use technology proactively much like the United States.

Unsurprisingly, other nations have chosen to take a proactive approach to national security. Advances in technology have allowed for the possibility to identify and contain terror threats in advance, as opposed to waiting for a major disaster to occur. September 11th was unique in that it spawned a global reaction; a change in policies in the United States also prompted a change in other areas of the globe, as well.

When it was exposed that the NSA was using PRISM to secretly gather intelligence, it was also revealed that the British government had some participation in this as well. Acting as a British equivalent to the NSA, the GCHQ had also been taking advantage the PRISM program for surveillance purposes.[26] Together, the NSA and the GCHQ utilized PRISM to mine vast amounts of data from American companies. Although the information being tapped in to was not being taken from British organizations, this is not to say that the GCHQ only gathered data regarding American citizens. Rather,

---

[24] Katrin Bennhold, Steven Erlanger, Ceylan Yeginsu, *Terror Alert in Britain Is Raised to Maximum as ISIS Claims Manchester Attack,* May 2017

[25] Laurel Wamsley, *ISIS Claims Responsibility For London Attack That Killed 7, Injured 48,* June 2017

[26] Barton Gellman and Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program,* June 2013

at the time, the United States acted as a hub for Internet activity, and as such, American companies held on to large amounts of data that could be used for intelligence purposes.[27] The concept of data mining on a large scale, therefore, was not strictly American; 9/11 may have begun a new age of counterterrorism for the U.S., but it spread to other areas of the globe increasingly concerned with the intentions of violent extremist groups. The British GCHQ was simply able to take advantage of the resources available to the American NSA, and the two countries collaboratively used PRISM as a tool against terrorism.

Another program put into action in the United Kingdom is called Prevent, which encourages citizens to speak up and inform authorities about suspicious behavior. The United States essentially has the same program, which is commonly referred to as 'See Something, Say Something.' These programs have raised privacy concerns, as critics note that citizens might be encouraged to 'spy' on their friends and neighbors as a result. Additionally, the program seems to have a disproportionate effect on Muslims.[28] As a result, the privacy rights of Muslims in particular are being compromised in the name of national security.

The United States and the United Kingdom share many similar antiterrorism programs, but interestingly, the United Kingdom actually has a more extensive framework of these policies than the U.S. Clive Walker, a legal expert on terrorism and an independent reviewer of the U.K.'s anti-terrorism legislation, claims that "the United Kingdom has some of the most extensive anti-terrorism legislation in the world which goes, I would suggest, far beyond anything you would find in the United States."[29] According to the United Kingdom's Liberty Human Rights Group, there are many Acts of Parliament that allow the government to act broadly against terrorism. The Civil Contingencies Act of 2004, for example, allows a Minister to enact emergency regulations whenever there is a threat of terrorism. Such regulations temporarily override any current legislation.[30]

To understand why this is, the difference in political structure between the U.S. and UK must be taken into account. The legal structure of the United States has largely been determined by the Constitution. Furthermore, the Democratic nature of the U.S. allows voters to choose representatives and more or less dictate the direction of public policy. These luxuries are

---

[27] Susan Landau, *Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations*, July/August 2013

[28] Scott Simon and Clive Walker, *U.K.'s Anti-Terrorism Programs Under Scrutiny*, May 2017

[29] Scott Simon and Clive Walker, *U.K.'s Anti-Terrorism Programs Under Scrutiny*, May 2017

[30] Liberty Human Rights Organisation, *Overview of Terrorism Legislation,* 2018

not universally enjoyed, however; in fact, "There is no written constitution in the UK. Instead, the rights of privacy and confidentiality of communications are protected under the Human Rights Act."[31] Without a Constitution, there are little inherent protections guaranteed to British citizens. As such, in the face of a temporary override of legislation, there is no standard of Constitutionality, giving the UK government substantially more discretion than the U.S. government. Additionally, decisions to allow infringement upon personal privacies outside of a period of emergency regulations are enacted by a politician in the UK, whereas in the U.S., permission to obtain search warrants and the authorization of surveillance comes from a judge.

There is some legislation in the UK that is similar to U.S. law. For example, the Telecommunications Act of 1984 is perhaps the closest piece of legislation to the American Patriot Act. Passed by Parliament, the Act gives the British government a lot of power with very little oversight: "[The Telecommunications Act of 1984] gives the government the power to issue 'directions' to providers of public electronic communications networks to do, or not to do, anything."[32] Unfortunately, the little oversight that exists fails to meet any standards of impartiality, as the commissioners charged with overseeing the process report to the Prime Minister. In other words, the commissioners do not work independently from the governing body they are tasked to oversee.[33]

In comparison to the United States, the United Kingdom has taken a restrictive approach to dealing with terrorism, but there is some evidence to suggest that it has been beneficial. On the following page, table 2 puts into context the level of activity seen within the United Kingdom since 2002.

---

[31] Douwe Korff, Ben Wagner, Julia Powles, Renata Avila, and Ulf Buermeyer, *Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes*, January 2017

[32] Douwe Korff, Ben Wagner, Julia Powles, Renata Avila, and Ulf Buermeyer, *Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes*, January 2017

[33] Douwe Korff, Ben Wagner, Julia Powles, Renata Avila, and Ulf Buermeyer, *Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes*, January 2017

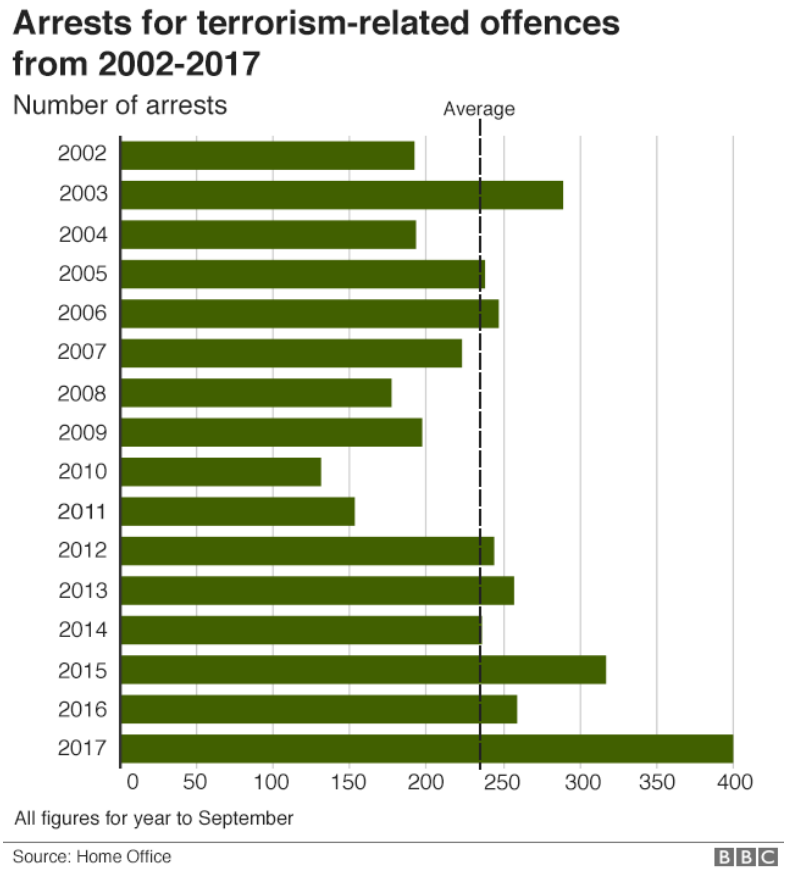


Table 2: BBC News, *Was 2017 the Worst Year for UK Terrorism?,* January 2018

According to this data, the average number of terror-related arrests have been higher in recent years, with a distinct peak in 2017. Admittedly, arrest statistics do not give a holistic picture of the scope of terrorism, as many arrested suspects are eventually released without charge. However, these statistics are also not arbitrary; rather, they give a sense of the approximate level of threat being dealt with by the UK on a yearly basis. From these numbers, it can be seen that the UK continues to combat a substantial amount of terrorism. Policing in the UK, whether it be due to surveillance through PRISM or programs like Prevent, has been at least somewhat effective in apprehending individuals linked to terrorism.

Most notable in Table 2 is the number of violent plots that were not successful. The official figure from the United Kingdom shows that 22 attacks have been foiled since 2013, with a staggering 9 being intercepted since only March 2017.[34] It is challenging to estimate the exact number of terror activities that have been prevented due to surveillance measures,

[34] Dominic Casciani, *Was 2017 the worst year for UK terrorism? ,* January 2018

especially due to the secretive nature of many investigations, but with at least 22 incidents prevented there is room to argue that the UK's strategies are indeed working. In light of legislation such as The Civil Contingencies Act of 2004 and the Telecommunications Act of 1984, however, concern over personal privacy remains separately from the relative success of surveillance and data mining.

Unlike the United Kingdom, the United States has recently been working towards rebalancing the scales of security and privacy. An example of this would be the USA Freedom Act of 2015[35], which "replaces the USA Patriot Act of 2001 [and] has made significant moves to protect the American people from bulk surveillance and data collection."[36] Admittedly, the U.S. has the upper hand when it comes to pro-privacy reform, as the Fourth Amendment to the Constitution already protects citizens from an unreasonable degree of interference from the government; something that the UK fundamentally lacks. Safeguarding the citizenry from abuse of government power was built into the American way of life from the inception of independence. The UK, while far from becoming a security state like that of historic East Germany, does not have the same built-in refuge from the overstepping of government.

## CONCLUSION

In order to have a free state, many components must work together in harmony. Security and privacy are two such components. Despite sometimes seeming to be at odds with one another, these two ideas do not necessarily need to be competing interests. Often, having a good foundation for one allows the other to blossom as well. However, a balance must be struck between the two in order not to overcompensate one way or another. Inherently, there will always be a struggle between the governing and the governed as each party attempts to gain additional power. In a way, privacy is one such power that a citizenry wields in the face of a governing body. Alternatively, the power to execute what is perceived to be good and necessary is something that the government wishes to have. As can be seen from the consequences of the Snowden leaks, governments occasionally take good intentions too far in this pursuit.

---

[35] *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA Freedom Act) Act of 2015, Pub. L. No. 114-23. The USA Freedom Act replaced the USA Patriot Act, which had expired. The Act was passed with great support in the House of Representatives, with a vote of 338-88 on May 13, 2015. The Senate then passed the Act with a vote of 67-31. President Barack Obama signed the Act into law on June 2, 2015.

[36] Andrew Murray, *Comparing Surveillance Powers: UK, US, and France,* 2015

Years after 9/11 and the Snowden leaks, it seems that many nations are at a crossroads when it comes to striking this balance. Those in the U.S. and the UK both realize it, but there is a large difference in the respective responses. Historically, terrorism in the U.S. has looked much different than what occurs in the U.K. The most major pro-security legislative reform in the U.S. came immediately following 9/11, whereas pro-security reform has existed in the UK for decades. Geographic proximity to many violent extremist groups has created a unique set of needs for the UK that the U.S. doesn't quite share. These factors come together to shape a distinct lack of pro-privacy reform in the UK like that of the U.S:

> The Federal Government of the United States has chosen to rein in some of the more egregious activities of its national security agencies, to restate the rule of law and strengthen the role of an independent judiciary, and emphasize the protections of the Fourth Amendment.[37]

The USA Freedom Act of 2015 exemplifies a desire of U.S. government agencies to reinvigorate the trust of the American people. National security remains a vital aspect of ensuring safety and comfort in the U.S., but the Snowden leaks have shown officials that illegal measures shrouded in secrecy can bring more harm than benefit. With terror-related arrests peaking in 2017 for the United Kingdom, there is a need for their government to reform certain strategies in order to ultimately rebalance personal privacies with more effective national security measures.

* * *

[37] Andrew Murray, *Comparing Surveillance Powers: UK, US, and France,* 2015