National Security, Mass Surveillance, and Citizen Rights under Conditions of Protracted Warfare

by

Krystal Lynn Conniry

A thesis submitted in partial fulfillment of the
requirements for the degree of

Master of Science
in
Conflict Resolution

Thesis Committee:
Rachel Cunliffe, Chair
Tom Hastings
Vandy Kanyako

Portland State University
2016

Abstract

This paper explores the complex relationship between securing the rights of citizens to privacy and national security priorities under conditions of government mass surveillance. The inquiry examines the conflict between those who support and those who stand in opposition of government surveillance, and is framed around the question of whether changes in technology and the concept of nationalism help inform our understanding of the increase in surveillance post-9/11. From a peace and conflict studies perspective, the work analyzes how the rise of nationalism in the post-9/11 era and the protracted wars against terrorism, in combination with the growth of technological power, have impacted the relationship between state-surveillance and democracy. Findings identify protracted warfare, technology and corporate profits as conflict drivers within the surveillance system, which gives rise to moral dilemmas and structural polarizations in the political culture and institutions of the state and society. The analysis concludes that these dilemmas systematically create an imbalance of power between the citizen to the state, and cannot be fully addressed unless the efficacy of war is critically questioned.

Acknowledgements

I would like to extend an enormous amount of gratitude and appreciation for the individuals in my life that have been conduits of support, encouragement, and love through this particular academic journey. This thankfulness extends to my caring friends and family, and the professors at PSU who challenged me through their knowledge and instruction. I would also like to mention my respect for the various individuals from whose work I drew from and upon which I built upon—allowing me to entertain and create new perspectives regarding the topic to be discussed.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

This study seeks to analyze the conflict between supporters of current government surveillance and those who oppose it. Where some supporters of heightened surveillance within the government justify the actions as necessary for national protection, others argue its legality simply due to the Executive orders that grant permission (Allen 2008; Frontline 2014; Toxen, 2014). Critics see the measures as a clear violation of certain Constitutional Amendments, particularly the First and Fourth Amendment. Government officials with such concerns, however, have been overruled, shut out, or in some cases indirectly requested to resign (Boghosian, 2013; Etzioni, 2015; Frontline).

The general public may have had more or less minor suspicions of government surveillance on American citizens. This discomfort became a full-blown concern in 2013 as a result of the Snowden revelations and what has been identified as an unprecedented breach of United States classified intelligence (Greenwald, 2014). Moreover, when NSA analyst Edward Snowden decided to leave his position and disclose thousands of classified documents that he had accessed while working for the NSA to media sources and journalists with the intention of exposing to the public the realities of what he came to know in regard to how the intelligence community conducts its tasks, it resulted in a national uproar with international repercussions. The extent to which the United States government had been utilizing technological resources and intelligence gathering mechanisms to conduct surveillance remains an issue of intense debate.

This particular topic became of interest to me when I was introduced to some of the ways in which companies and corporations share and transfer personal information in an effort to increase sales and become more efficient in regard to consumer targeting

efforts. When the Snowden revelations and the issue of electronic mass surveillance became a hot topic of debate, my inquiries around personal privacy then evolved into an interest in the relationship between human rights to privacy and national security. Drawing from my studies of nationalism, protracted warfare, and the technological implications deriving from a globalized economy, I began to wonder if and how these elements could possibly be contributing to the surveillance phenomenon. With this said, my inquiry has been framed around the question: How do changes in technology and the concept of nationalism help inform our understanding of the increase in surveillance post 9/11? In the attempt to explore the structural and contextual aspects of this question it became quite clear that the issue of government surveillance and personal privacy is a complex one with several interrelated and intersecting factors. To present my findings in a fitting and understandable way, I have organized the rest of the paper as follows:

In Chapter 2, I focus my attention on the growth of surveillance post 9/11. I identify the most significant legislative measures regarding US surveillance leading up to 9/11 and those after. This chapter also presents related data ranging from surveillance trends, to public opinion, and to the relationship between government surveillance and the information technology industries.

Chapter 3 explains my strategies of inquiry. This includes the types of resources I used, where I got them, and why I chose them instead of others. It was my intention to identify the leading voices from both sides of the surveillance debate, while allotting particular attention to sources that may have presented connections between surveillance, nationalism and technology.

Chapter 4 provides a conflict analysis of the surveillance debate post 9/11. In this chapter, dominant themes and arguments of both the pro-surveillance advocates and the anti-surveillance advocates are presented. There is also a section dedicated to the analysis of the growth and power of technology. It includes public opinion polling data on how the government's data collection program is perceived as well as government intrusion of personal privacy in the advent of investigating terrorism.

In Chapter 5, the discussion section, I introduce the following elements: the growth and power of technology, protracted warfare, and the rise of nationalism in the post 9/11 era. These three elements, and their interrelatedness, has not been sufficiently taken into account when it comes to the surveillance debate. For example, the ways technology has and continues to grow outside the frameworks of the law, the social and psychological impacts of warfare and violent conflict, and the often willing-sacrifice of personal freedoms to authoritarian and government measures under crisis conditions.

In Chapter 6, I present implications, limitations and directions for further research. This chapter summarizes the complexities and controversies deriving from post-9/11 surveillance measures and how the relationship between national security and human rights is currently in a state of ambiguity. In this chapter, I highlight the impacts of technology, warfare and nationalism with regard to the surveillance issue and stress that these dynamics create imbalances of power between the citizen and the state that cannot be fully addressed unless the efficacy of war is critically questioned.

Chapter 2: Growth of U.S. Surveillance Post-9/11

The four coordinated terrorist attacks targeting both New York and the Pentagon on September 11th 2001, constituted a historical turning point and heralded an unprecedented augmentation of national security efforts both within and outside the United States. With wide-spread citizen support and internal pressures regarding the safety of America and its citizens, the US took immediate action in what was branded the "War on Terror," a term coined by former president, George W. Bush.

In addition to the US invasion of Afghanistan on October 7, 2001, which would later evolve into America's longest-standing protracted conflict in history, legislative measures were quickly taken, with the expressed intention to protect and prevent the nation from ever experiencing attacks such as those on 9/11 again. The most significant of these measures was the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act," also known as the USA PATRIOT Act, which made several changes to US law, including, but not limited to, laws pertaining to immigration, banking, diplomatic espionage, and electronic mass surveillance conducted both domestically and abroad (Bamford, 2008; Boghosian, 2013; MacAskill, 2013 Peissl, 2003; Smith & Hung, 2010). This level of intrusion on private lives was a significant departure from what had gone on before.

Background of US Surveillance

Legislative acts and measures regarding US surveillance can be dated as far back mas the country's conception, but took dramatic turns in the early 20th century in the advent of communication advancements and the onset of the two World Wars. During World War I, with the increased use of radio technology for military operations, the US

created the Cipher Bureau with the Military Intelligence Division, to assist with radio intelligence and cryptology—the study of codes and how to crack them. Although the bureau was disbanded in 1929, it was reestablished as the core of the Signal Security Agency in World War II (McNiff, n.d.). The first law formally addressing wiretapping was the Federal Communications Act of 1934 and established the Federal Communications Commission (FCC). Under this Act, wiretapping was not considered illegal, however the information that was gathered was protected under a nondisclosure agreement (FCC).

In addition to propelling US engagement into World War II, the unexpected attacks on Pearl Harbor in 1941 contributed immensely to America's heightened surveillance measures and the transformation of US military intelligence agencies. In 1947, the National Security Act was passed, creating the Central Intelligence Agency (CIA) and the National Security Council to combat "new threats to American security" (Gallagher, 2013). In 1949, the Armed Forces Security Agency (AFSA) was created within the Department of Defense, which was responsible for organizing electronic communication throughout civilian agencies. It was in 1952, however, that President Harry Truman issued a memo transforming the AFSA, due to critiques of its ineffectiveness, into the National Security Agency (NSA). According to the memo, the purpose of the NSA was to create an efficient and organized system of control over the communications intelligence activities of the United States against foreign governments (Gallagher).

The Cold War era marked another transformative period for US surveillance and intelligence-gathering agencies. In light of global communication advancements after

World War II, along with Soviet fear and the potential use of nuclear weapons, the primary focus of the NSA continued to be gathering and decoding as much information as possible from real, or perceived, threats to the nation. The extent to which the NSA could go in pursuing these goals was governed by the extent to which these communications were electronic, and the extent to which the NSA could intercept and decrypt them (Friedman, 2014). It was not until 1968 that the first federal law, the Omnibus Control and Safe Streets Act, to restrict wiretapping was passed by Congress in 1968 (Gallagher, 2013; McNiff, n.d.; Vicens, Gilson, & Park, 2013).

The Watergate scandal in 1972, and President Nixon's impeachment for attempted wiretapping and the seizing of secret documents, raised national awareness and concern with regard to government practice and Executive use of electronic eavesdropping. Pressures for reform within the political arena mounted, with a call for more transparency (McNiff, n.d.). With regard to national surveillance, however, the NSA remained relatively unknown to the American public (Cohn, 2013).

It was in 1975, during the course of a US Senate and intelligence-gathering investigation lead by Senator Frank Church and the so-called Church Committee, that many Americans learned that not only did the NSA exist, but that it had been conducting surveillance on American citizens (Cohn, 2013; Debenedetti, 2013; Gallagher, 2013). Moreover, the investigation uncovered hundreds of cases where the CIA and FBI had conducted warrantless wiretappings and unauthorized electronic surveillance. In defense, the Director of the NSA testified that the Agency was only monitoring "anti-Americans" for the purposes of identifying foreign criminals (Gallagher).

In response to national concerns following the Watergate and Church revelations, in 1978, Congress brought forth the Foreign Intelligence Surveillance Act (FISA), which was signed into law by President Carter (Debenedetti, 2013; Gallagher, 2013). The Act established guidelines for the use of foreign intelligence surveillance, and authorized the creation of secret FISA courts to request warrants for electronic surveillance related to national security. Moreover, it determined that the only circumstances under which the US and its intelligence agencies could lawfully conduct electronic surveillance would be for the purpose of collecting foreign intelligence or foreign counterintelligence (Debenedetti).

As a response to the commercialization of computers, as well as technological advancements in wireless and data communications, an amendment to the Omnibus Crime Control and Safe Streets Act of 1968 was introduced, called the Electronic Communications Privacy Act (ECPA), in 1986, which extended government restrictions on wiretaps to include cell phone and internet activity (Debenedetti, 2013; Gallagher, 2013). The Act also added new provisions with regard to the access of stored electronic communications (McNiff, n.d.; Vicens et al, 2013). The most drastic of transformations in US surveillance came in the wake of the 9/11 terrorists attacks and the endorsement of the USA PATRIOT Act, which has had an immensely controversial and sustained global impact.

The USA PATRIOT Act greatly expanded the US government's authority to use surveillance domestically and internationally and removed many of the previous restrictions that had been set into place, for the protection of personal privacy (Peissl, 2003, Smith & Hung 2010). Among other provisions, the Act authorized the use of

electronic mass surveillance on American citizens and the storage of personal data, while also reducing the checks and balances of judicial oversight and public accountability (Boghosian, 2013; Byman & Wittes, 2014; Etzioni, 2014; Greenwald, 2014; Peissl; Smith & Hung).

The most significant changes to the scope of legal surveillance under the USA PATRIOT Act are (1) the ability for government powers to capture and retain personal records from third parties including doctors, libraries, bookstores, universities, and Internet providers (Section 215); (2) the expansion of the government's ability to search private property without providing notice to the owner (Section 213); (3) the ability for the FBI to secretly perform physical searches and wiretaps on American citizens with the intent to obtain evidence of a crime without probable cause (Section 218); and (4) the expansion of a Fourth Amendment exception for spying that reduces judicial oversight and interprets "addressing" information in a way that authorizes the tracking and accumulation of personal URL activity and Internet content material (Section 214) (Smith & Hung, 2010; USA PATRIOT Act). An illustrated timeline regarding the background of US Surveillance (beginning in 1934) can be found in Appendix A. For now, we will observe some of the statistical trends and patterns of surveillance post-911.

Trends and patterns of surveillance

The controversy over state surveillance in the post 9/11 era has generated a wide array of data on related issues ranging from surveillance trends, to public opinion, to corporate roles. Such data comes from reputable polling agencies, such as the Pew Research Center, the Washington Post and ABC News Poll, the Wiretap Report to

Congress from the Administrative Office of U.S. Courts and the American Civil Liberties Union (Abdo, 2013).

The data delivered by the above-mentioned polling agencies cluster in three main domains, first general trends in state surveillance; secondly, the role of corporate service providers; and finally, trends in public opinion. The first two will be addressed in this chapter and the trends in public opinion will be presented in Chapter 4.

Data on general trends in state surveillance

Figure 1 displays data from a 2007 Wiretap Report to Congress from the Administrative Office of U.S. Courts. State and federal wiretapping authorizations are shown by year of issue.

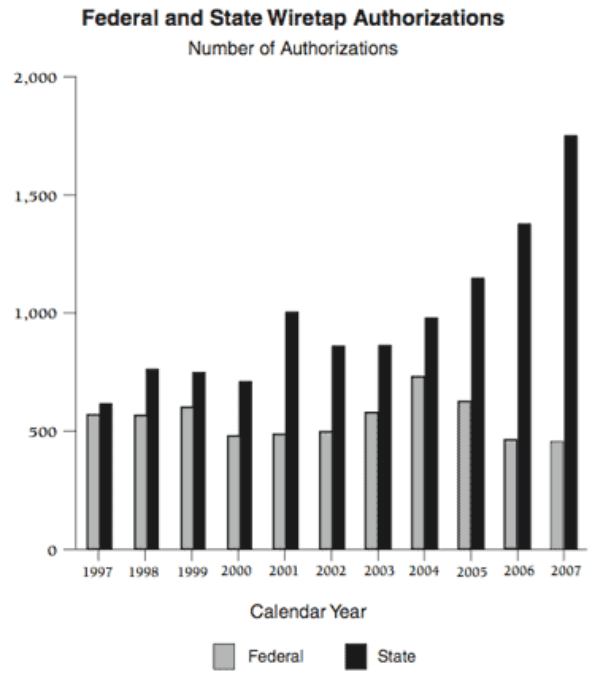


Figure 1: Federal and State Wiretap Authorizations. Retrieved from Singel, R. (2008, May 1). Court-Approved Wiretapping Rose 14% in '07. Retrieved April 05, 2015, from https://www.wired.com/2008/05/court-approved/

While the form of surveillance shown here is not among the most secretive, it reveals a sharp spike in state wiretap authorizations in the post 9/11period. This report also indicates significant increases of state wiretap authorizations from 2004 to 2007. What is important to note about government wiretapping reports, and what researcher Julian Sanchez states well is that "these numbers don't include Foreign Intelligence Surveillance Act wiretaps, 'pen register' requests for communications metadata, or orders to acquire stored e-mails sitting on a server" (Sanchez, 2010, para. 1). Meaning that these particular statistics do not take into account the vast majority of electronic communication that happens over the Internet such as email, Instant Messenger, Twitter, Facebook and the like.

The trend toward increasing government surveillance became more apparent with news about the Secret Court of the Foreign Intelligence Surveillance Act (FISA), which authorizes surveillance that is not disclosed to the public. According to a 2011 report by the ACLU:

> The government more than *quadrupled* [sic] its use of secret court subpoenas, known as 215 orders, which give the government access to "any tangible thing," including a wide range of sensitive information such as financial records, medical records, and even library records (Greene, May 9, 2011, para. 2).

The ACLU report also talks about the secret court's issuing of the so called National Security Letters (NSLs), which gives government wide range access to sensitive information such as financial records, medical records, library records and others. It stated that:

> There was also a substantial increase in NSLs, which allow the FBI to demand records related to a broad range of personal information, including financial records, a list of e-mail addresses with which a person has corresponded, and even the identity of a person who has posted anonymous speech on a political website, all without the permission or supervision of a court. In 2010, the FBI *more than doubled* [sic] the number of U.S. persons it surveilled with NSLs, requesting 24,287 NSLs on 14,212 people, up from 14,788 NSLs on 6,114 people the year before. The FBI also increased its electronic and physical surveillance, making 1,579 applications to wiretap and physically search individuals' property last year, up from 1,376 the year before (Greene, May 9, 2011, para. 3).

Again, the overall trend is toward increasing government surveillance. Figure 2 shows the number of surveillance orders issued by the US government from 1998 to 2012:

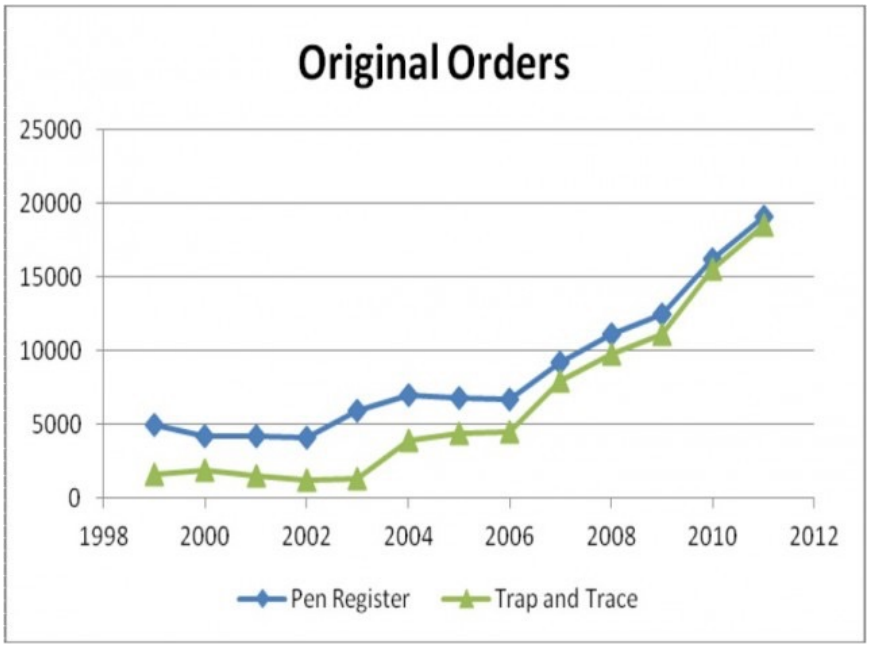


Figure 2: Surveillance Orders Issued by the U.S. Government, 1998 – 2012. Retrieved from Gilen, N. (2012, September 27). New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance. Retrieved June 4, 2015, from https://www.aclu.org/blog/new-justice-department-documents-show-huge-increase-warrantless-electronic-surveillance

Figure 3 shows the number of people affected by the above-mentioned government orders:

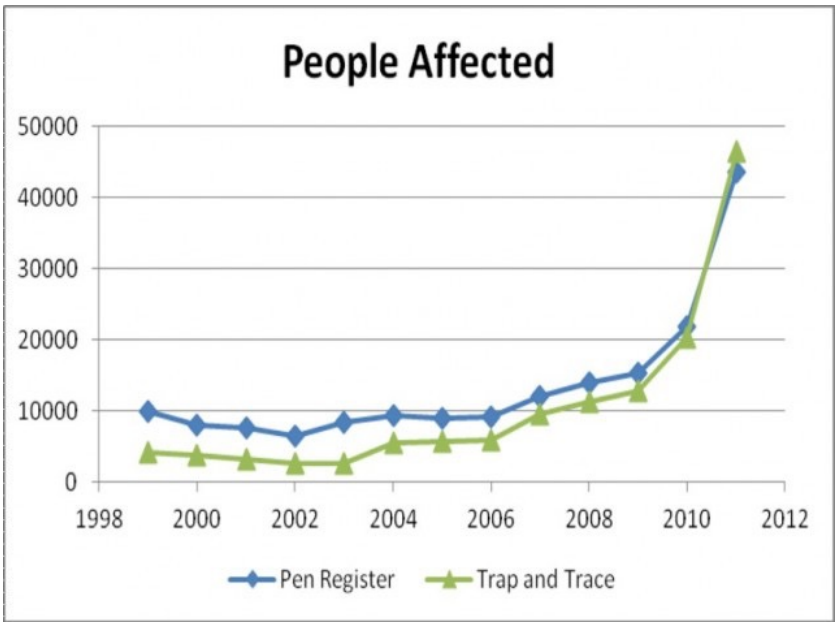


Figure 3: People Affected by Surveillance Orders Issued by U.S. Government, 1998 – 2012. Retrieved from N. G. (2012, September 27). New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance. Retrieved June 4, 2015, from https://www.aclu.org/blog/new-justice-department-documents-show-huge-increase-warrantless-electronic-surveillance

Figure 4 displays statistics on e-mail and Internet surveillance during the years 2003 to 2012. The term Pen Register refers to outgoing electronic inquiries, phone calls, emails, and URL searches. Trap and Trace techniques are those that collect and store similar information, but that are incoming to the personal user or ID (Abdo, 2013).

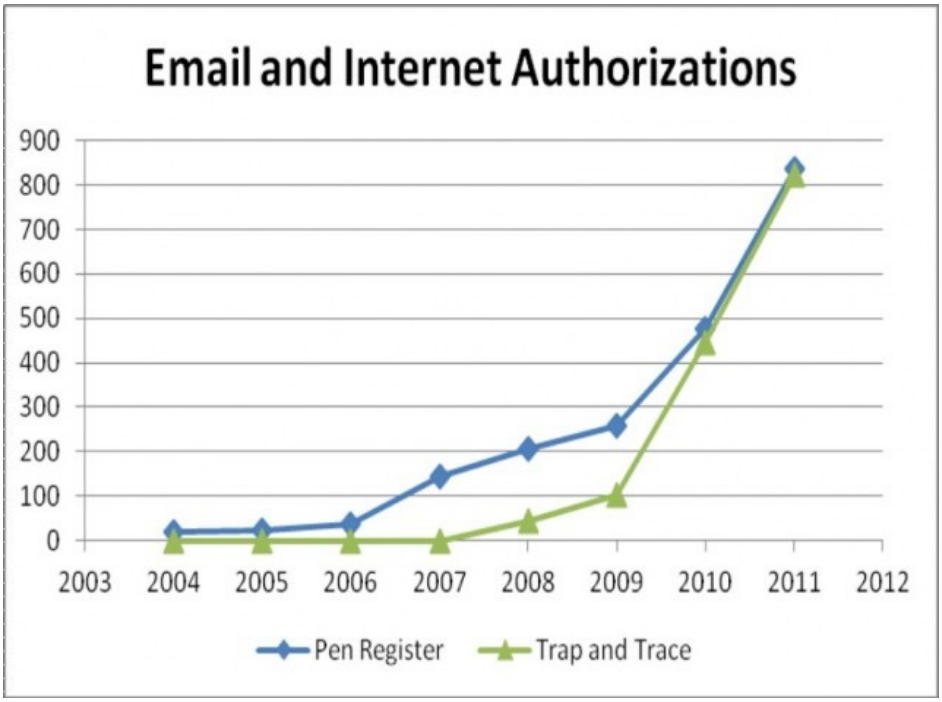


Figure 4: Statistics on E-mail and Internet Surveillance, 2003 – 2012. Retrieved from N. G. (2012, September 27). New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance. Retrieved June 4, 2015, from https://www.aclu.org/blog/new-justice-department-documents-show-huge-increase-warrantless-electronic-surveillance

Figures 2, 3, and 4 were published in 2012 after the ACLU forced the US government to reveal certain surveillance statistics. The ACLU revealed that the Federal government had collected more phone records over the previous two years than during the previous ten years combined. It was also noted that these statistics were likely only a fraction of the surveillance being conducted, as much was classified and could not be accessed by the ACLU. As the ACLU notes, their data do not include:

> …cell phone location tracking law enforcement. They also omit government access to emails stored by third party providers. And they entirely exclude the National Security Agency's warrantless wiretapping program under the FISA Amendment Act. While hard numbers are hard to obtain, what little evidence we

do have suggests that all of these forms of surveillance have been increasing (Lee, September 27, 2012, p.8)

Under the pressure of the Snowden revelations, the Obama Administration was compelled to disclose some (but not all) of the government's secret activities in a report released in June 2014. The report indicated that in 2013, 19,212 NSLs were authorized by the FISA secret court thus enabling the FBI to collect information without a warrant. Again, the available data indicates a strong trend toward increased government surveillance (Lee, 2012)

In the post 9/11 era, government surveillance has also tended to intrude in the area of financial surveillance. Data indicate that under national security considerations government surveillance of financial records has vastly increased. Data from the Treasury Department that were released in 2011 show that financial surveillance of people by the United States government hit an all-time high with the number of suspicious activity reports rose 13.5 percent to 1.5 million from 2010 to 2011 (Cook, 2012). Critics suggest that financial surveillance is an overreach beyond monitoring terrorism and that much of the legislation currently being enforced with regard to surveillance, is a retraction from the earlier measures intended to protect citizen privacy in a digital era.

The Privacy Act provided safeguards for citizen privacy with relation to government and financial institutions (The USA PATRIOT Act, 2001). The act also granted individual citizens the right to access information that private and public institutions held about them, with the ability to correct any errors. In addition, government and corporations were obliged to keep the information safe and organized, using it only for lawful purposes. Similar conditions pertained to the Fair Credit

Reporting Act of 1970. Standards for encrypting personal data were also established (McNiff, n.d.). As early as 1977, The National Bureau of Standards required encryption procedures to the protection of computer data, particularly with regard to financial transactions. By 1993, the Clinton administration ushered into the system new and more powerful encryption standards developed by the NSA (Freeman, 1995).

The introduction of the so-called Clipper Chip was central to the new standard. Using a powerful algorithm, the chip was a semiconductor that was designed to be installed in all computer modems, fax machines and telephones to encrypt communications data (Freeman, 1995). As early as 1977, particularly in regard to financial transactions, The National Bureau of Standards required encryption procedures for the protection of computer data (Freeman). However, built into these encryption mechanisms were secret government keys, which allowed government officials access to this personal information. In this context, although encryption laws promote citizen privacy, there is the paradoxical component in which the government is able to quickly unlock this information if desired. And as security measures heighten, the concentrated power that these master keys represent are placed in the hands of fewer and fewer people.

The Role of Corporate Service Providers

The next category of data relevant to the present inquiry concerns the part played by corporations and specifically by service providers from the information technology industry in the growth of surveillance post 9/11. The principal security technologist in the Privacy and Technology Project of the American Civil Liberties Union (ACLU), Christopher Soghoian, noted that there is a close relationship between government surveillance and the information technology industry of the private sector (Soghoian,

2009). Soghoian stated that Internet firms and telecommunications carriers receive monetary compensation from the government when they disclose customer information to law enforcement officers (Soghosian). Soghoian also stated that:

> Cox Communications, the third largest cable provider in the United States, is the only company I've found that has made its surveillance price list public. Thus, we are able to learn that the company charges $2,500 for the first 60 days of a pen register/trap and trace, followed by $2,000 for each additional 60 days, while it charges $3,500 for the first 30 days of a wiretap, followed by $2,500 for each additional 30 days. Historical data is much cheaper -- 30 days of a customer's call detail records can be obtained for a mere $40. Comcast does not make their price list public, but the company's law enforcement manual was leaked to the Internet a couple years ago. Based on that 2007 document, it appears that Comcast charges at least $1000 for the first month of a wiretap, followed by $750 for each month after that (December 1, 2009, para. 28).

Data suggests that the involvement of the private sector information technology industry in government surveillance has been on the rise (Greene, 2011; Soghosian, 2009). This information was disclosed by The Washington Post on June 6, 2013 when it published information on PRISM, an electronic mass surveillance program initiated by the US government in 2007 that works in conjunction with telecommunications companies to monitor and store various forms of electronic communications both domestically and abroad. The information gathered above does not require individual warrants, since it has broad approval by the secret FISA court. Published by the Washington Post (June 7, 2013).

Figure 5 shows the timeline and identity of each of the nine Internet companies that participate in the government surveillance program. It also notes the price tag of the PRISM program at $20 million per year.

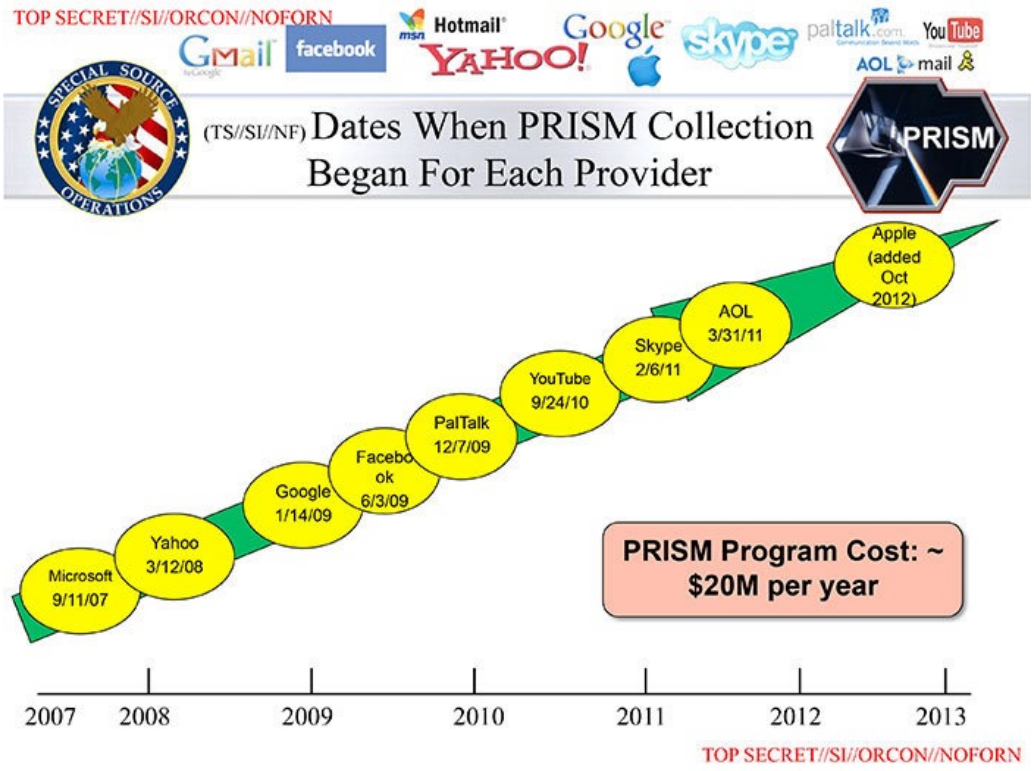


Figure 5: Relationship Trends of Government, Private Sector and Information Technology Companies. Adapted from Gellman, B., & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. Retrieved May 29, 2016, from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

When focusing on data reflecting the involvement of private sector, information technology industry in surveillance, the trend reveals a rise in the intensity and breadth of government surveillance by also involving the corporate private sector, which has a corresponding financial interest in participating.

The data discussed in this chapter shows a marked increase in quantity, scope, and depth of intrusion into private lives by government surveillance either directly or through purchase from other organizations and providers. Where organizations have expanded their services to include harvesting and selling personal data, they clearly have a financial interest in technological innovation to secure their competitive advantage.

So while the facts are undisputed, their meaning is at the center of considerable conflict in both academic and popular culture. This study seeks to explore that conflict and understand what drives it.

Chapter 3: Strategies of Inquiry

As stated in Chapter 1, my inquiry has been framed around the question: How do changes in technology and the concept of nationalism help inform our understanding of the increase in surveillance post 9/11? In this context, and against the backdrop of the history of US surveillance, the research and analysis focuses on the post-9/11 era, when surveillance came to the forefront of mainstream media. It addresses the USA PATRIOT Act that was signed into law shortly after the terrorist attacks in 2001 and examines the effects this act has had on the surveillance state and the government's executive powers. The inquiry also draws from contrasting positions of prominent authors, academics, journalists, government officials, and filmmakers relevant to the surveillance debate. My intent was to identify the structural and contextual components of the debate that suggest competing perspectives on and assumptions underpinning the issue of surveillance.

Positioned within the theoretical framework of peace and conflict studies, the research and analysis presents new information and insights from the social sciences for a more comprehensive and intelligible understanding of the issue at hand. The analysis section highlights the evolution of information technology and the rise of nationalism and the protracted wars post 9/11. The inquiry assesses whether these two factors impact and condition the surveillance phenomenon, and if so, how. In investigating these factors, this study claims to add a new and original component to the surveillance debate. Using this framework in the attempt to explore the terms and context of the surveillance debate I used three primary sources of data. These sources are listed below and a list of the dominant authors from whom I drew my research with regard to the pro-and-anti-surveillance perspectives can be found in Appendices B and C.

Primary Sources

1. Consultation with experts: The primary expert that I spoke to was Dr. Harry Anastasiou, who has taught and written extensively on the subjects of nationalism, protracted conflict, and technology.
2. Library resources: I followed up my discussions with Anastasiou with an extensive search of peer-reviewed literature and reports using a combination of key terms such as human rights, privacy, technology, nationalism, national security, warfare, protracted conflict, democracy, security, and government surveillance.
3. Popular culture best sellers: I then reviewed popular culture for comment on the subject, focusing particularly on best-seller lists and some of the most prominent news sources.

Strategy of Analysis

Once I had identified my sources I read and annotated, attending particularly to the connections I had identified and according to a conflict analysis strategy. A conflict analysis strategy is one that identifies, observes and analyzes the profile, causes, actors, and dynamics of a particular conflict in an attempt to have a more comprehensive perspective of the issue, so that appropriate levels of intervention can be determined and implemented (Melander, Bengtsson, Ekstedt, & Holmberg, 2006). This kind of approach looks for ways to establish systematic linkages and synergies between causes and factors within particular, and in some cases, more abstract conflicts. This type of analysis strategy also encourages the researcher to have a mix of perception-based and objective indicators that can be measured through both qualitative and quantitative methods.

Following the directives associated with performing this type of analysis (Melander, et al.), I worked off of the following questions in an effort to understand the structural and contextual elements of the surveillance issue:

- What is the primary focus and nature of this conflict?
- Who are the actors and what is their position?
- What are the common themes voiced by pro-surveillance and anti-surveillance advocates?
- What are the interests behind this position?
- What (if any) shared meaning exists between protagonists?
- Are there implicit assumptions, which are not brought to the surface?
- What structural asymmetries are present in this debate?

Once I had identified the most apparent characteristics and profile of my particular topic I began recording both qualitative and quantitative trends, themes, positions and perspectives from the various actors involved. (Actors referring to all those engaged in or being affected by the conflict.) As I continued to study the conflict, using the aforementioned questions, I noticed a very complex system of interrelated factors and dynamics influencing the surveillance debate.

The first chapter of findings presents the nature of the conflict. The second chapter presents the debate's context, structure, and the drivers that keep it going. The last chapter will conclude with the implications, limitations, and suggestions for further research.

Chapter 4:
Conflict Analysis on Human Rights and Crime Control

The disciplinary field of peace and conflict studies (PCS) is one that seeks to understand the cause and effects of both large and small-scale conflicts in addition to the preconditions for peace. Although inquiries into the reasons for war and the nature of peace can be traced all throughout human history, the emergence of PCS as a distinct scholarly discipline began in the early 20th century, coinciding with World War I, and gained much momentum soon after World War II (Barash & Webel, 2014). With its incorporation of theories and research from the fields of anthropology, sociology, psychology, political science, economics, ethics, theology, and history, PCS has been identified as possessing a multi-and trans-disciplinary dimension. PCS is also multi-leveled, as it encompasses peace and conflict evaluations on the interpersonal, intergroup, and international levels—whether in the context of friends, family, communities, organizations, ethnic groups, states, or civilizations (Barash & Webel, 2014). At its core, PCS aims to analyze the root causes of conflict and the psychological and structural frameworks of both individual and collective violent and non-violent behavior, with the intent to apply its findings in a transformative way that promotes peace, reconciliation, nonviolence, and the prevention of war. This chapter employs a conflict analysis strategy to illuminate the nature of the surveillance debate.

Writing on the surveillance issue appears to be sharply contrasted between those who strongly support surveillance practices of the US government and those who strongly oppose it. A variety of genres are used to communicate a broadly similar message across a variety of audiences. However, certain voices emerge almost as

spokespeople above a foundation of support. In each of the camps the authors range from analysts, to journalists, to politicians to legal experts.

Pro-Surveillance Advocates

Some of the most prominent supporters of surveillance included the following: the Bush administration, attorney Gerald Walpin, journalist and senior producer at CNBC Mathew J. Belvedere; Secretary of State John Kerry; former Secretary of Defense Robert M. Gates; and Republican Speaker of the House John Boehner. What all of these and others have in common is that they associate their position of support for surveillance by the federal intelligence community to the war on terror.

Particularly in the post-9/11 era, pro-surveillance advocates have argued that it is not only constitutional, but also necessary for America's intelligence community to deploy the most up-to-date technology to monitor electronic communications, both internationally and domestically (Allen, 2008; Blankley, 2008; Inkster, 2014; Lomas, 2014; Toxen, 2014; Walpin, 2013). For example, Nigel Inkster, former director of operations and intelligence for the British Security Service states that, "the US is operating its own interpretation of the law, as it is enshrined to, citing the imperative of national security" (p. 53). Pro-surveillance advocates have further claimed that hi-tech surveillance and intelligence gathering is a very powerful tool that has enabled the US government to identify, and effectively prevent terrorists from attacking America, and, as such, support that electronic surveillance should continue and expanded if able (Allen; Blankley; Lomas).

It has also been argued in the pro-surveillance community, that for surveillance and intelligence gathering to be efficient and effective, especially with regard to

preventing terrorist attacks, it should be unimpeded (Blankley, 2009; Lomas, 2014; Walpin, 2013). For example, Gerald Walpin, former Inspector General of the Corporation for National and Community Service, reflects the argument well when stating:

> That enemy exists, the evidence for it consisting of 3,000 lives lost on 9/11, the Boston Marathon massacre, and even the unsuccessful terrorist attacks on our airplanes and at Times Square. The NSA program is logical. Our intelligence people know phone numbers or area codes used by terrorists in various world locations. Wouldn't you want our intelligence services to know who in the United States called those numbers and area codes and to examine the information to determine whether those calls were innocent or not? I certainly would. If this program had been applied to identify the Boston bombers, that attack could have been prevented (para. 8).

In addition, Walpin suggests that the logic underpinning this position is that any attempts to place intelligence gathering bodies such as the National Security Agency (NSA) and its affiliates under some form of civil oversight, through a full-time civil liberties and privacy officer, is an unrealistic and contradictory endeavor. Moreover, Walpin (2013) claims that any such attempt would hinder intelligence activities and make it more difficult to combat our already difficult war on terrorism.

Therefore, pro-surveillance advocates appear to see anti-surveillance advocates as ideological, naïve and out of touch with reality. More importantly, it appears that many surveillance supporters perceive anti-surveillance advocates as demagogues threatening government security efforts in their advocacy of individual rights to privacy (Walpin, 2013). By implication, pro-surveillance advocates view anti-surveillance advocates as

gravely dangerous to national security, and/or as traitors, whose position and actions in attempting to disclose and limit the government's surveillance capabilities, amounts to aiding and abetting the enemies of America (Belvedere, 2014; Dann, 2014; Epatko, 2014; LoGiurato, 2013; Toxin, 2014; Walpin).

Anti-Surveillance Advocates

Authors who oppose state surveillance agencies and their respective programs base their position on a shared premise arguing that surveillance by the US government has reached such extreme levels that it threatens democracy in general, and the democratic rights of American citizens (Boghosian, 2013; Cassidy, 2013; Frontline, 2014; Gellman & Poitras, 2013; Greenwald, 2014). Critics of state surveillance include authors such as: journalist for the New Yorker John Cassidy; author and former journalist for The Guardian, Glenn Greenwald; author, journalist, and Pulitzer Prize recipient Barton Gellman; former Foreign Intelligence Surveillance Court (FISA) Judge John D. Bates; former intelligence analyst Edward Snowden, among others.

In opposition to the pro-surveillance advocates, many anti-surveillance advocates view government surveillance, particularly in light of current revelations, as an overreach, abuse, and violation of governmental power that threatens democracy and the rights of American citizens (Boghosian, 2013; Frontline, 2014; Gellman & Poitras, 2013; Greenwald, 2014). Many premise their position on the principal idea, as articulated by Abraham Lincoln and the American constitution of "government of the people, by the people, and for people." For example, in the first lawsuit brought against the NSA regarding warrantless wiretapping in 2006, District Court Judge Anna Diggs Taylor ruled in favor of the American Civil Liberties Union stating that, "the NSA program was

illegal, violating both FISA and the Fourth Amendment of the Constitution" and that "It was never the intent of the framers to give the president such unfettered control, particularly when his [George W. Bush] actions blatantly disregard the parameters clearly enumerated in the Bill of Rights" (Bamford, 2008, p, 290). Similar to Taylor, several anti-surveillance advocates assert that, as the cornerstone of democracy, the sovereign rights of the people should be protected and assume priority over any demands or expectations regarding the actions of the state and government (Boghosian; Frontline; Gellman & Soltani; Greenwald).

In addition, anti-surveillance advocates contend that the extent to which the US government has been engaging in surveillance, both domestically and internationally, is unconstitutional and a violation of human rights, particularly with regard to citizens' rights to privacy (Bamford, 2008; Boghosian 2013; Etzioni, 2014; Gellman & Soltani, 2013; and Greenwald, 2014). They argue that unimpeded mass surveillance is more or less ineffective in preempting terrorist attacks—arguing that more surveillance does not lead to more security, as the ever increasing amounts of mass data that is collected puts the intelligence community in a situation where they are essentially looking for a needle in a haystack (Boghosian; Etzioni). Moreover, the secrecy under which the state's intelligence programs operate erodes the citizen's right to know what the state is doing on their behalf, thus eroding government transparency as one of the cornerstones of democracy (Boghosian; Cassidy, 2013; Greenwald; Klein, 2013).

Glenn Greenwald, a prominent literary figure within the anti-surveillance community, and the initial receiver of Snowden's classified documents, has written explicitly on what he states as "the dangerous trends in US state secrecy, radical

executive power theories, detention and surveillance abuses, militarism, and the assault on civil liberties" (2013, p.14). Greenwald goes on to describe US secrecy and non-transparency as a one-way mirror, in which the government has limitless power to see what the world around them is doing, while no one can see its own actions.

Heidi Boghosian, another powerful voice among anti-surveillance literary figures, expresses considerable concern with regard to the relationship between freedom and democracy when coupled with "relentless surveillance" and the potential impacts that surveillance could have on American society (2013, p. 22). These concerns are summarized well when she states that:

> "Rather than advancing freedom and equality, inescapable surveillance enforces a form of authoritarianism that undermines both. It degrades the ability of members of society to challenge and organize against government and corporate injustices. The loss of cultural freedom stifles individual creativity and the unfettered community interaction necessary to keep power in check and to advance an evolving society" (p. 12).

Similar concerns have been raised by advocates within the anti-surveillance community and have suggested that such surveillance could lead to adapted forms of human behavior including a particular loss of autonomy, in which individuals refrain, either consciously or subconsciously, from acting and behaving in ways that are more true to their own unique personalities, and more in accordance with how they are expected to be perceived by governmental and societal expectations (Boghosian, 2013; Cassidy, 2013; Frontline, 2014; Gellman & Soltani, 2013; Greenwald, 2014; Klein, 2013; Peissl, 2003). Peissl likens this adaptation in human behavior to the "panoptic society,"

where if individuals have the awareness that societal surveillance structures have been put into place, but have no idea when they are or when they are not being monitored, there is an automatic power shift that takes place between those observing (in this case the US government) and those being observed (civilian participants). Those supporting this view express that this loss of autonomy in democratic societies would more than likely have negative societal and economic outcomes (Boghosian, 2013).

Other concerns with regard to US government actions in the realm of state surveillance include beliefs that the federal government misleadingly uses national security surveillance for diplomatic espionage and economic influence, and that the spying on national allies, and the potential impacts of future exposures, may have harsh repercussions with respect to international relations (Hakim, 2014; Traynor, 2013). Anti-surveillance activists also promote strong distaste for current government-corporate partnerships, which they proclaim to only strengthen and solidify the misuse of government power (Boghosian, 2013). Perhaps the most severe criticism that this group levels against the pro-surveillance group, is that the State's extent of domestic and international surveillance, and its enormous capacity collecting and storing massive amounts of information on leaders and citizens, as well as the sheer concentration of power in amassing such amounts of information, begins to approximate the features of an authoritarian totalitarian state (Boghosian).

Legal experts are similarly polarized on the legality and constitutionality of the issue at hand. In his book *The Supreme Court vs. The Constitution*, Gerald Walpin (2013), a prominent attorney who served as Inspector General for the Bush Administration, strongly argued in favor of the constitutionality of government

surveillance, as a vital instrument for fighting terrorism. In 2011, Federal Judge John D. Bates, was at that time serving as chief judge on the Foreign Intelligence Court that was to oversee the activities of the NSA, and who was known to authorize much of the agencies activities. In an 85-page ruling, Bates concluded that in its secret foreign surveillance program it had run over the previous years, the agency has violated the Constitution, as it was conducting warrantless surveillance domestically. Furthermore, Bates identified the problem as part of a pattern of misrepresentation by agency officials in submission to the secret court (Savage, 2013).

Although, numerous voices among political leaders and citizens refer to the need to strike a balance between surveillance and privacy, the above mainstream positions strongly suggest that national security considerations and democratic human right considerations are moving in divergent directions. In fact, it appears that the relationship between those who are concerned with security and those who are concerned with human rights is a polarized one.

Court Cases and the NSA

As mentioned above, legal experts are polarized on the legality and constitutionality of the issue at hand. There have been several lawsuits against the practices of federal surveillance agencies by political leaders as well as by civil society organizations. For example, in February 2015, Kentucky Senator Rand Paul (joined by former Virginia Attorney General Ken Cuccinelli and FreedomWork's Matt Kibbe), filed a class-action lawsuit against the Obama administration and the NSA's meta-data program, arguing that the current warrantless wiretapping being conducted is a violation of individual rights as stated in the Fourth Amendment (McCalmont, 2014). Paul, who

has also been a strong opponent of the USA PATRIOT Act since its commencement, criticized the government's ability to search, indiscriminately, the phone records of Americans. Paul aims to see this case brought before the Supreme Court where there can be a public argument about whether the Fourth Amendment does indeed apply here. In this context, Paul claims there is an unequal and subjective nature to this debate because, as of yet, it has taken place primarily between government officials and representatives of the NSA, without citizen participation. According to Paul, this environment, with the majority consisting mostly of those working for the US government, will be more inclined to promote the continuance of surveillance for the sake of national security (McCalmont).

In March 2015, the Wikimedia Foundation, along with eight other rights groups, filed a lawsuit against the NSA and its mass electronic surveillance tactics, stating that it violates privacy rights and makes individuals worldwide less likely to disclose sensitive information (Ingram, 2015). Co-founder of Wikipedia, Jimmy Wales, claims that the company was specifically targeted for "upstream surveillance" (a term often used to refer to the collection of data along the so-called backbone of the Internet through fiber-optic cables, and away from individual users) and that they have evidence that the company has endured harm due to the released Snowden documents (Ingram). The ALCU's report regarding this particular case stated that "upstream surveillance hinders the plaintiffs' ability to ensure the basic confidentiality of their communications with crucial contacts abroad – among them journalists, colleagues, clients, victims of human rights abuses, and the tens of millions of people who read and edit Wikipedia pages" (Davies, 2015).

U.S lawyers, with expertise in defending national security measures, have referred to the litigation claims as a "long shot" for the Wikimedia foundation, and accompanying rights groups, based on the difficulty in sufficiently proving harm done by the NSA. Anyway, government spy agencies are usually able to halt such hearings by arguing the need to protect State's secrets (Ingram, 2015). These court cases are currently in progress and their final outcome, as of yet, remains unpredictable.

The table below provides a summary of the contrasting major themes in the literature review of the anti- and pro-surveillance advocates, respectively:

Table 1: Dominant Themes of Surveillance Debate post-9/11

Themes of Pro-Surveillance Advocates	Themes of Anti-Surveillance Advocates
State surveillance is constitutional and necessary in averting terrorism	State surveillance in unconstitutional and unnecessary in averting terrorism
Surveillance is a powerful tool of the government that effectively prevents terrorist attacks	Surveillance does not lead to more security and is not effective in averting terrorism
Surveillance must continue to expand unimpeded in the war against terrorism	Surveillance reflects extreme government overreach
Surveillance must be both international and domestic	Surveillance has reached unlawful levels domestically and internationally
Anti-surveillance advocates are out of touch with reality, naïve and gravely dangerous for national security	Surveillance enhances government secrecy that undermines democratic transparency
Anti-surveillance advocates are traitors who aid and abet the enemy	Surveillance leads to the authoritarian state threatening democracy and human rights

The comparison of mainstream perspectives on the issue of surveillance provides a useful starting point for the conflict analysis. The contrasts also prompt important questions as to what the underlying reasons are for why and how these contrasting perspectives are formed. Structural and context analysis may help illuminate these

differences, as well as a more comprehensive depiction of how the power and growth of technology influences the surveillance issue.

Growth and Power of Technology

Against the entire backdrop of the polarization and controversy over surveillance, the power of technology, and more specifically, of information technology and its role in surveillance behavior, has rarely been taken into account in the mainstream debate. Opinion and literature within the social sciences has often promoted technology, and the information revolution in particular as a pro-democracy instrument. The highlighted benefits are that it allows citizens to exchange and share ideas, to communicate in unimpeded ways beyond any government's capacity to control and sensor, to disclose corruption and injustices around the world, and hold political leaders accountable. However, authors who have studied the growth of technology from a critical perspective have argued that, along with many benefits, technological advancement has posed significant challenges to democracy, the rights of citizens, and the function of the law in relation to the power of technology (Castells, 2010; Freeman, 1995; Scott, 2012). This is a matter that, as of yet, has not been sufficiently addressed within the current surveillance controversy. A prerequisite for addressing this issue is a basic understanding of the mode of technological advancement and diffusion into society.

As early as the 1960s and 1970s, seminal thinkers analyzing the growth of technology, such as Jacques Ellul, Alvin Toffler, Lewis Mumford, and George Grant presented arguments with regard to technological growth and advancement. Their perspectives noted that uncritical faith in technological progress in the modern era imparts, to technological developments, an unchecked and unquestioned autonomy that

often leads to technology contradicting and even violating the non-technical spheres in society, such as ethical considerations, the rule of law, the democratic process, institutional transparency, the labor market, citizen rights, and nature itself with environmental degradation and recently, climate change. Moreover, both Ellul, in his works *The Technological Society* and *The Technological System*, and Mumford, in his two volume piece *The Myth of the Machine*, noted early on that the spectacular expansion and growth of technology in its modern form does not occur primarily through the work of geniuses, but rather through the work of thousands of very ordinary specialized technicians who make largely unnoticeable, incremental, improvements (Ellul, 1967; Mumford, 1971). However, Ellul and Mumford also both argued that it is not the innumerable individual technical improvements that bring about socially impactful innovations, but the way in which the technologies intersect, interact, and combine into highly efficient complex systems, whether circumstantially or by design.

These perspectives become even more compelling when considering current world conditions. The advent of the so-called 'Information Society,' and the general rise of the 'Digital Age,' are characteristic and universal in the post-modern world, and have bequeathed an unprecedented dependency and fixation on the preservation, progression, and expansion of technological development and advancement. For example, as a relatively new phenomenon, with its commercialization in the early 1990s, the global system of interconnected IP systems, also known as the Internet, has become so embedded in contemporary societies that it is difficult, for many, to imagine what life would be like without it. Moreover, in advanced societies, there is hardly an organization or institution whose functions are not structured in and through the digital process of the

ethereal and extraordinarily abstract and intangible universe of cyberspace. Analysts such as Castells (2010) have spoken of the rise of the 'Network Society,' asserting that the digital world, and the Internet in particular, has established electronic interconnections within societies as well as interconnections globally. He argues that this global electronic networking has established a global technological system that functions as a new infrastructure of the world. It is this networking system that seems to have vastly empowered the capacity for surveillance.

In light of the above, it appears that the autonomy of technological growth, when facilitated by an unquestioned acceptance of technology, and the incremental and minute ways in which thousands of technologies evolve and systemically combine, renders the gradual yet enormous impact of technology as "natural" and thus unnoticeable (Ellul, 1967; 1980). Perhaps one of the most central and yet neglected phenomena at the heart of the so-called surveillance state, pertains to the abstract, intangible, and enormously complex digital system that, in nature, is unapproachable, and the cyber-world in which such digital structures reside. For the ordinary citizen, the complex and the unapproachable are incomprehensible. More specifically, this is seen in societies that are deemed as having democratic systems of governance (Grant, 2011)—one of the more apparent examples being the United States, which is arguably the most technologically advanced society in the world.

With this said, it is important to address the continuity of technological capacity between the private and public sectors. Many scholars of the surveillance phenomenon have commented on the ways in which technology is currently operating erases the distinction between sectors by imparting the same capacity to both corporations in the

private sector and the state in the public sector (Boghosian, 2013; Greenwald, 2014, Gellman & Poitras, 2013; Soghoian, 2009). Moreover, the technological systems that have substantially increased the capacity for massive data collection, storage, manipulation and utilization are so integrated and systemically interconnected that one can no longer differentiate where the private sector begins and the public sector ends (Boghosian; Greenwald). For example, when the NSA utilizes data from private sector service providers such as Google, Yahoo, Facebook, AOL and others, they are operating through a single, extended and seamless technological system, where the distinction between the private and the public sector has become effaced and largely meaningless (Soghoian).

Under these conditions, the growth of technology, particularly information technology, gradually outgrows the framework of the law, creating new phenomena while the law increasingly lags behind (Ellul, 1967; Toffler 1991). The capacity of corporations to hold and utilize enormous amounts of personal data and information about clients and consumers, and the capacity of the state to collect, store and utilize multiple categories of data on their own citizens as well as on citizens of other countries, has led libertarians and civil rights advocates to push for legislative changes in an effort to protect personal data and citizen privacy (Etzioni, 2015). However, scrutiny of the existing laws reveals a considerable imbalance, whereby the human rights protected by law are superseded by the capacity of technology used by the state and corporations to elusively operate at the edge of the law and even beyond the law (Freeman, 1995; Givens, 2013).

In his article entitled “When Technology and Privacy Collide,” Edward H. Freeman noted that:

> Civil libertarians consider computer and communications technology to be a serious threat to individuals’ personal privacy and freedom of speech. Some advocate laws to provide both an effective legal basis for accountability in the handling of personal data and procedures for redressing and compensating individuals. The development of the information superhighway may compromise personal privacy even more (1995, p.41).

What should be noted here is that critics of the intrusion of information technology on citizens’ rights to privacy, find recourse in the law as the instrument that will give citizens protection while holding accountable those who manage the information systems. As concerns mount, government agencies, civil libertarians and the computer industries contribute to the enactment of laws to protect citizen privacy rights. This trend, which coincided with the advent of computers and electronic communications in the second half of the 20th century, gave rise to two related forms of legislation. One involved laws that specifically identified and protected the privacy rights of citizens in regard to their personal data held by government and corporations, such as the Freedom of Information Act (Banks, 2010), the Privacy Act, and the Fair Credit and Reporting Act (Freeman, 1995). The other entailed the development and incorporation into law, methods of data encryption by which electronic messages would be coded and decoded accordingly by persons who were legally authorized to do so. An example of the latter would be the Clipper Chip that was previously mentioned.

Although often neglected, but of great significance with regard to the evolution of standards for protecting citizen rights, is that the enacted laws rendered electronic messages more secretive and inaccessible, except to authorized persons. Corporations and government inadvertently become holders of secret master keys for coding and decoding the masses of encrypted data (Frontline, 2014; Gellman & Soltani, 2013; Greenwald, 2014; Mears, 2014). Paradoxically, all of the aforementioned protections served to expand the sphere of secrecy on the side of corporations and government. In other words, the more secure the systems become through encryption the more secretive the government and corporations can be. Meanwhile more power becomes concentrated and centralized at the top ranks of the information management systems, and knowledge of the secret codes and access to the huge data banks becomes accessible to fewer and fewer individuals within the relevant institutions, whether public or private (Lomas, 2014).

Another vital issue then comes to the forefront. It is the fact that in advanced societies, technology, in contrast to the law, grows at geometric rates (Friedman, 1995). Technology, with its dynamic capacity to innovate and expand through the interactivity of its elements and its interconnecting systems, vastly accelerates technological growth and, subsequently, its tremendous impact on society. The law, on the other hand, evolves and grows at arithmetic rates, and is thereby much slower in responding to challenges, including those that technology introduces (Ellul 1967; 1980). Hence, the accelerated rates of technological growth outpace the corresponding growth of the law. As a result, the relationship between technology and the law is one where the law is continually trying to catch up with its speedy counterpart. According to Ellul, even when the law

does attempt to address the technological phenomenon, rather than furnishing democratic and legal management over the power of technology and its likely intrusions into the fabric of democracy and human rights, its evolution appears merely to adjust and accommodate technological growth.

Along with the benefits that come out of technological advancement, what is often overlooked is that the trend mentioned above, as well as other technological trends, tends to move away from democracy, not toward it (Ellul, 1967; 1980). Yet, the uncritical belief in the power of technology, in combination with the belief that we live in developed democracies, tends to suppress the contradiction between the aforementioned aspects of information technology and democracy, especially privacy rights.

The table below provides my summary of the features of information technology that have increased the capacity for surveillance:

Table 2: Key Features of Information Technology with Relation to Surveillance

Technological advancement benefits but also challenges democracy and human rights
Uncritical faith in technology allows technology to develop unchecked
Some technologies may evolve in contradiction to democracy, transparency and the rule of law
Technological growth takes place incrementally and unnoticeably through thousands of small specialized steps
Information technology has become a new global infrastructure interconnecting the world
Technologies grow globally through interaction and interconnections into complex systems
Technologies create the infrastructure of the “network society” nationally and globally
Computer technology has vastly increased the power of government and corporations
Technology creates a seamless continuity between public and private sectors of society
Technology vastly increased the capacity to collect, store and manipulate information
Corporations and government managing and protecting huge information systems entail secrecy

Systems of information technology are complex, intangible, abstract and inaccessible to ordinary citizens
Computer technology in a digital age is a new system of power challenging privacy rights
Technological advancement tends to outgrow the law as it evolves at greater speed than the law
Human rights and privacy protected by the law tend to be superseded by the advancement of technology

The categories of technology listed in table 6 strongly suggest that the power of digital technology has played a role in facilitating the polarization between the pro- and anti-surveillance advocates, as the power of technology has shifted power disproportionality from the citizens to the state and corporations. The categories of technology also help explain the vast increase in state surveillance, as the growing power of technology allows for, (a) the unprecedented massive collection, storage and manipulation of information; (b), a seamless digital interconnectivity between state surveillance and the storage banks of private sector service providers; and (c) a tacit acceptance of the growing power of technology by public opinion due to the incremental, dynamic and synthetic way in which technological growth takes place, evading sufficient democratic scrutiny.

The power of technology has provided the infrastructure and the means for greatly increasing the capacity for surveillance. As Ellul suggests, technology is an ambiguous and complex phenomenon that cannot be classified as solely good or solely bad. However, this ambiguity and complexity should promote special attention to the impact of technological innovation.

In the context of protracted wars since 2001, and the perpetual fear of terrorist attacks, the power and context of national security-driven surveillance in the digital age has reached historically unprecedented heights. The novelty of the phenomenon is underpinned by the technological capacity of US intelligence agencies to intrude into the electronic communication networks, practically anywhere in the world and to collect, store, and process information. Although most citizens would typically object to such personal intrusion via these technological capabilities, when in the midst of crisis conditions and the fear of terrorist threats, public opinion appears to be more accepting of government measures that invade personal privacy (Clark, 2013).

Trends in public opinion

Perhaps the most extensive polling on public opinion about surveillance was published in 2013 by the Research Center, one of the most reputable polling agencies. The following figure reveals how public opinion views government surveillance.

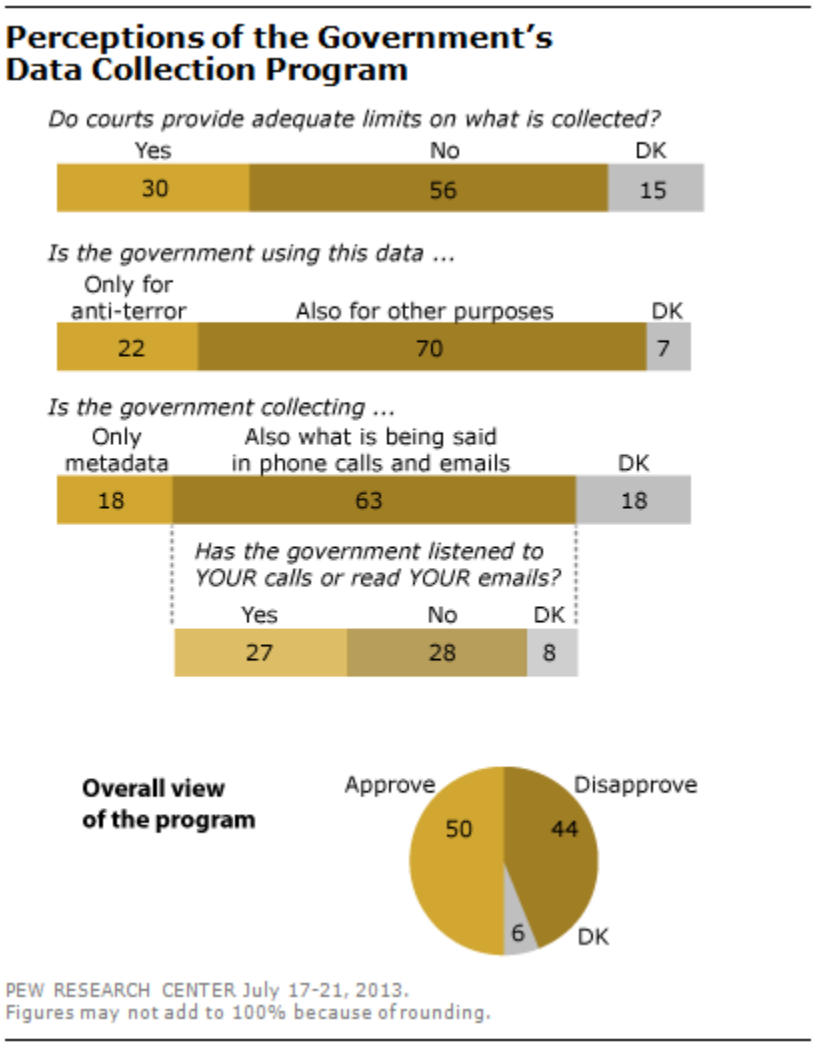


Figure 6: Perceptions of the Government's Data Collecting Program. Adapted from Dost, M. (2013, July 25). Perceptions of Government's Data Collection and Views of Program. Retrieved April 30, 2015, from http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/4-perceptions-of-governments-data-collection-and-views-of-program/

What is interesting is that while the majority believes (1) the courts do not provide adequate limits to government surveillance; (2) that government uses the information it collects for purposes other than for anti-terrorism; and (3) that the government is also collecting the content of citizens' phone calls and e-mails, the majority still approves of government surveillance. While apparently paradoxical, this is an indication that public

opinion is also moving in the direction of accepting increasing government surveillance, despite the arguments made by the anti-surveillance advocates.

Figure 7 affirms the mandate the public is apparently giving the government for its surveillance program.

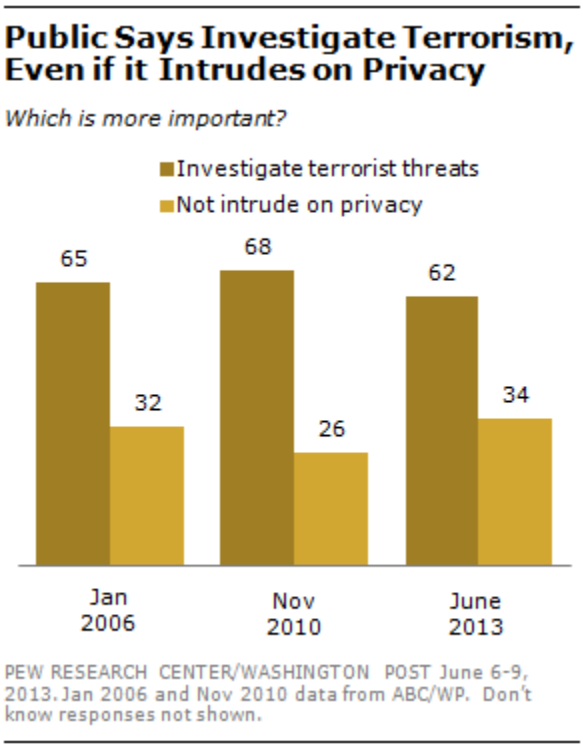


Figure 7: Public Opinion in Relation to Terrorism and Personal Privacy. Adapted from Clark, M. P. (2013, June 10). Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic. Retrieved April 30, 2015, from http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

Here again, while the majority opinion is that government surveillance is intrusive and not sufficiently regulated by the courts, the majority simultaneously believes that surveillance targeting terrorism is more important than the right to privacy or a requirement for government transparency.

In this context, we see the unique contest between human security and the human right to privacy under conditions of protracted warfare, crisis, and uncertainty. More

specifically, we see how the majority of citizens are willing to sacrifice personal freedoms to privacy when there is a real and/or convincing threat to the security of the nation. For example, in the aftermath of the 9/11 attacks, and particularly during the run-up to the Iraq War, US surveillance focused not only on specific enemy targets, but also on unprecedented targets, or targets without proper justification (Frontline, 2014; Greenwald, 2014). American intelligence agencies, in cooperation with British intelligence, was monitoring, among others, the communications of UN weapons inspector Hans Blix, the UN Security-General Kofi Annan, and UN delegations of six countries as part of a campaign intended to apply pressure on these countries to vote in favor of using force against Iraq (Payne & Shah, 2013). There is also evidence that during the Bush administration, the US Central Intelligence Service entered into a surveillance partnership with Libyan dictator, Muammar Gaddafi (Payne & Shah). The agreement was that the US would spy on Libyan dissidents in the west in exchange for permission to use Libya for extraordinary renditions—the transfer, without due process, of a detainee to custody of a foreign government for purposes of detention and interrogation, which might involve torture.

If the state develops the capacity and willingness to conduct surveillance on diplomats and UN officials, who presumably are not deemed as enemies of America, it is easy to imagine how much more aggressive, intrusive and expansive state surveillance may be in monitoring actual or potential terrorists. The central issue here is that in its very efforts to intercept and preempt Islamic militants from attacking Americans at home and abroad, the US intelligence community, using its sophisticated electronic surveillance instruments, has been compelled to cast the broadest possible net to make sure it catches

anyone who intends to harm America and/or its allies (Bamford, 2008; Blankley, 2009; Greenwald, 2014). The assumption is that the broader the net the more effective the intelligence community is in preempting terrorist attacks (Greenwald). Conversely, the narrower the net, the greater risk of missing critical intelligence. The argument appears to go that the more comprehensive and more total the data collection is, the closer to technologically foolproof the national security system will be.

Critics from the pro-democracy and human rights camp object to the approach of the intelligence community by arguing that broad surveillance tactics erode democracy and are less effective in catching the culprits, as the sheer mass of data collected results in looking for a needle in a gigantic haystack (Boghosian, 2013). Effective surveillance, argue the pro-democracy advocates, needs to be narrowly focused, with oversight and a transparent legal process authorizing surveillance warrants for specific and identifiable suspects.

The counter view of the more nationalistic and technologically empowered pro-surveillance advocates among political leadership, the intelligence community, and the citizenry is that as the surveillance agencies now have the capacity to collect, store, and classify an effectively infinite amount of information, they should do so. If then, a suspect is identified, they will subsequently have the ability and legal right, to digitally retrace that individual's communications activities to the greatest possible detail. The central idea here is that the broad and even indiscriminate collection and storing of data, enables the surveillance agencies to digitally store "reality" in the sphere of electronic communications (Frontline, 2014). As a result, they can subsequently digitally reproduce that reality so as to be able to go back and retrace the activities of suspects, once they are

identified. If data is discarded, or its collection is legally restricted, then the surveillance agencies lose the advantage of going back to stored data and retroactively examining the communications of individuals and groups once they are deemed suspected criminals or terrorists.

Chapter 5: Protracted Warfare, Nationalism, Technology and Corporate Profits as Conflict Drivers

This chapter explores the context and structure of the surveillance debate. In an attempt to understand particular conflicts it is necessary not simply to understand roots and causes. Nor is it sufficient to attend only to their content. Conflicts frequently exist in systems with multiple interrelated and intersecting factors affecting their trajectory and intensity. Understanding structures and dynamics within such systems is of primary importance in conflict analysis.

Structurally the surveillance debate puts individual rights to privacy against collective rights to security. However, when analyzing the conflict more deeply these positions reveal contested territory with respect to a notion of security. On the one side, security is thought to be derived from protection by military might from others from whom we are separated, and on the other, the focus is on respect for individuals and the power of trusting connection.

Unfortunately, such debates are frequently prolonged and become what Kriesberg (1998) has called intractable conflicts or what Ramsbotham (2011) has called radical disagreements. Protagonists speak past one another other by setting different problems to solve. The fact that the other side does not engage with the problems that are brought to the surface, facilitates judgment and opposition. This dynamic is evident in the surveillance debate. Anti-surveillance advocates view pro-surveillance advocates as abdicating citizen responsibility to an overreaching government, particularly with respect to individual rights to privacy. Meanwhile individuals within the pro-surveillance camp, see their opposition as naïve because they do not engage or take into account the real and potential dangers of terrorist attacks (Blankley, 2009; Inkster, 2014)

The structural element of this conflict is the vast power and influence of corporate interests supporting technological innovation, a market of data collection and storage, combined with protracted warfare and big government, which renders the debate asymmetric. The context of this conflict is framed within this set of structural relations. There are several intersecting forces within this context. The power of technology has been discussed at length in the previous chapter. In this chapter I explore nationalism and protracted conflict. I then discuss the respective and collective influence of both nationalism and protracted conflict and technological innovation with regard to the surveillance phenomenon.

Rise of Nationalism and Protracted Conflict in the post-9/11 Era: Crisis, War, and Democracy

Scholars of nationalism, mostly non-Americans, agree that in response to the 9/11 attacks, American politics and society came under the influence of aggressive nationalism. They also agree that the rise of American nationalism in the post 9/11 era motivated the global war on terror and greatly shaped American domestic and foreign policy, as well as public opinion (Anastasiou, 2011; Lieven, 2004a; McCartney, 2004) Since surveillance is frequently justified in the context, it is important to consider the characteristics of nationalism.

The most notable experts on nationalism assert that there exists a close relationship between social and political crises, warfare and nationalism (Alter, 1994; Howard, 1994). In times of crisis, when countries engage in warfare, nationalism emerges as a dominant force. This certainly appears to be the case in America following the tragic, unexpected attacks of 9/11. The literature also indicates that nationalism endorses

warfare, creating a culture where war is viewed as legitimate, necessary, and even moral (Alter; Anastasiou; 2008; 2011; Anastasiou & Broome 2010; Howard; McCartney, 2004). McCartney notes that American nationalism in the post-9/11 era viewed America's wars as a moral mission to save America and humankind from the evil of dictators and terrorism.

All the above-mentioned authors have a critical view of American nationalism. Tony Blankley (2009) on the other hand, an American author who identifies himself an American nationalist, fully supports American nationalism, considering it a worldview that is necessary for the survival of the nation. For Blankley, it appears that the value and status of the nation is absolute and should be of utmost priority. In looking at the challenges that America faces, he describes attachments to citizen privacy rights as selfish, and that the interest of the nation should be first and foremost.

Critical authors note that nationalism requires and demands national unity, expecting all citizens to collectively support the state when it goes to war. Moreover, these authors argue that the influence of nationalism increases the power of the state over its citizens in the name of national security (Anastasiou, 2008; 2011; Lieven, 2004; McCartney, 2004). The question that arises is whether the increasing powers of the state that nationalism sees as legitimate in times of war, have had an impact on the growth of state surveillance in the post 9/11 era.

The multiple protracted wars that the US and its coalition partners initiated in response to the attacks of 9/11 have, in effect, complicated the issues surrounding the protection of citizens' democratic rights, especially rights pertaining to personal privacy (Givens, 2014; Peissl, 2003). Although it is not uncommon for citizens' to consent to

temporary breaches of certain human rights under conflict conditions, or the threat of attack, it appears that the technological mechanisms that have been created and implemented under conditions of protracted conflict, mixed with nationalistic fervor, have in many ways become an almost unstoppable system now deeply embedded in today's society (Givens). Analysts have observed that the years following 9/11 and the US-led global war on terror have complicated international affairs in many ways, one of which is the privileging of the power of the state and the undervaluing of human rights and civil liberties in the interest of national security (Patton, 2006).

As a historical pattern, states, when under conditions of crisis, especially when at war, become driven by a defensive-aggressive reaction to increase control over any phenomena (Anastasiou, 2008). This includes domestic or foreign control that may be seen as posing an actual or potential threat. In the name of national security and of protecting the citizens of its national community, in most cases, the state assumes increasing powers (Savage, 2013). It does so either by acting at the edge of the law, or by enacting emergency laws that provide the legal grounds for doing so, and, if need be, by acting outside the law in extra constitutional ways premising such actions on a higher necessity (Banks).

Citizens, on the other hand, tend to react to conditions of crisis, especially when the country enters war, through fear and uncertainty, which activate and amplify the instincts of vengeance, aggression and survival (Matiya, 2013). Analysts such as Givens (2013) and Rubin (2011), note that, under these conditions, citizens tend to move toward increased trust in government authorities especially in the immediate wake of terrorist attacks. Furthermore, is it argued that popular support of government in times of crisis

provides the political capital necessary for legislators and executives to quickly craft and implement anti-terrorism laws that may undermine democratic rights (Givens; Rubin). As this dynamic takes root, citizens tend to seek refuge in consolidating the national community and supporting the leadership nearly unconditionally. For example, the popular opinion and citizen support of the offensive and defensive measures taken and/or proposed by the Bush Administration that closely followed the terrorist attacks of 9/11 (Immerman, 2011).

In this evolving pattern, citizens become more complacent with regard to reductions of human rights, and more tolerant to authoritarian measures and approaches by their government and state. As Allen (2008) states, "A significant number of Americans believe that to effectively combat terrorism, it may be necessary to infringe on civil liberties" (p. 591). Simultaneously, governments experience populist approval for taking on more powers and for acting in increasingly authoritarian ways. Thus, because it is grounded in broad collective fear and uncertainty, the emergence of the authoritarian surveillance state tends to be readily accepted by the public (Anastasiou, 2010). This dynamic gives a semblance of a democratic system when in reality it is more of what one may describe as a populist and consensual regime of authoritarianism (Boghosian, 2013). Here one can easily argue that the rise of nationalism in times of war permits the state to resort to the unrestrained, unimpeded, use of technological power.

Drawing from experts such as Anastasiou, Broome, Alter, Lieven, and McCartney, Table 3 provides my summary of the primary features of nationalism that have increased "legitimacy" and acceptability of state surveillance:

Table 3: Key Features of Nationalism according to Anastasiou, Broome, Alter, Lieven, and McCartney in Relation to State Surveillance

Features of Nationalism
In times of political crisis and warfare, nationalism emerges as a dominant force
Nationalism endorses warfare as legitimate, necessary and even moral
Nationalists see the nation as having an absolute value, above all else.
In nationalism and warfare the interest of the nation is higher than human rights
Nationalism requires and demands national unity with all citizens supporting the government and the state
In response to the attacks of 9/11 America's leadership and mainstream society turned towards an aggressive nationalism
American nationalism endorsed the "war on terror" as a moral mission to save America and humankind
Consequences and Impact on the State
Nationalism and warfare increases the power of the state over its citizens in the name of national security and interest, especially in times of war
Under nationalism and warfare, the state is inclined to make full use of technological power, which increases the power of the state
Nationalism and warfare privileges the power of the state, while devaluing human rights and civil liberties in the name of national security and national unity
Under nationalism and warfare, state power tends to act at the edge of law, enact undemocratic laws, or act outside of the law in the name of national security, as a higher necessity
Consequences and Impact on the Citizens
Under nationalism and warfare, fear, uncertainty and the need for security tend to move citizens toward increasing trust in government authorities, especially in the wake of terrorist attacks
Under nationalism and warfare, citizens tend to seek refuge in national unity under the power of the state
Under nationalism and warfare, citizens tend to become acquiescent in relation to their government, while political leaders feel empowered to legislate undemocratic, emergency measures in the interest of national security
Under nationalism and warfare citizens tend to become more complacent in regard to human rights and more tolerant to authoritarian measures and powers assumed by government and the state

I would argue that the interaction of nationalism and protracted warfare has a powerful influence on the phenomenon of increasing surveillance, and that this interaction has been essentially overlooked in the debate over surveillance. As nationalism, argued by the experts in this field, endorses warfare and the necessary political, legal and extralegal measures that prioritize national security, it increases the power of the state (Anastasiou, 2011), and with it, I would argue, the prerogative of the state to conduct surveillance through the full use of technological power, especially at a time of war. It appears that under the impact of nationalism and warfare, fear, uncertainty and the need for security on the part of the citizens, compels citizens toward increasing trust in government authorities, finding refuge in the power of the state.

In this context, state surveillance tends to become a priority of the state and is generally acceptable by citizens (Givens, 2013). The movement toward increasing state power, including state surveillance, helps explain in a more comprehensive way, the position of the anti-surveillance camp and its rivalry against the pro-surveillance advocates. The impact of nationalism and warfare also helps to further contextualize and explain the data trend in surveillance, specifically that (a) there is an increase in state surveillance; (b) that the state engages collaboratively the private sector service providers to conduct surveillance as the state prioritizes national security; and (c) that public opinion tends to accept the state's extraordinary measures, including surveillance, even if they are seen as intrusive to citizen privacy.

It appears that under conditions of war, coupled with persisting terrorist threats and actual attacks, it has been deemed by the more nationalist-minded among the leadership and citizenry as most effective to proliferate data (Walpin, 2013). It is this

approach that gave rise to the new concept in the world of surveillance, now commonplace in the media and public debates, namely *meta-data.* Meta-data refers to information that describes and categorizes arrays of other bodies of information (Schneier, 2014). In other words, it is data derived from categorizations, organization, and analysis of other data, which makes finding and processing specific categories of data easier. Based on the idea of meta-data, the advocates of aggressive and expanded surveillance argue that sweeping masses of data does not amount to spying because those who manage intelligence systems do not analyze the data, but simply harvest and store the data under particular categories for future reference when it is necessary and/or legally warranted (Schneier).

Once this high-tech approach is absorbed and "normalized" by the nationalist paradigm, the compulsion to move the system in the direction of ever extended sweeps of data gathering appears in the eyes of nationalists as both necessary and preferable. Intertwined with a history of Jihadi threats and attacks, America's continuing engagement in protracted warfare and special operations around the world, leads nationalists among Americans to the position that expanding the scope and capacity of surveillance globally serves national security and the national interest (Lieven, 2004a).

As projected from the state, the prime focus of surveillance and data gathering on specific enemy groups and movements is for the purpose of preempting terrorist attacks (Byman & Wittes; 2014). However, having developed the technological capacity of gathering and storing massive amounts of metadata surveillance activity goes far beyond the identifiable vowed enemies of America, to include anyone who may in the future become identified as a suspect (Greenwald; 2014). Under this scenario, any person,

government, group, or organization from around the world may be included. This approach illustrates a kind of preemptive surveillance that can, and may, encompass any individual and any population around the globe. While democracy-minded leaders and citizens may question the state's authority for such extensive reach, the nationalist-minded leaders and citizens see it as a legitimate projection of national power, since their inviolable and superiority view of their own nation, place the latter above all other nations and above any international standard or accountability (Lieven, 2004a; McCartney, 2004). Here one sees how the absolutist notion of national sovereignty, purported and sustained by nationalism in combination with the optimal projection of technological power, can create the very anarchic international conditions that the realist theory of international relations, in which aggressive uses of raw power to uphold state supremacy are condoned and prioritized, finds its self-justification (Anastasiou, 2008; 2011; Barash & Webel, 2014). In this way, nationalists fail to critically understand that the anarchic world they invoke is not necessarily a given, but the byproduct of nations and movements acting through sheer power and outside any framework of international law or normativity (Anastasiou, 2011; Korab-Karpowicz, 2010; Lieven; McCartney).

While shocking to many, the news that broke in the international media in October 2014, very much reflected the logic of the above described system, as it was reported that within a period of thirty days the NSA had swept up to 70.3 million telephone records of French citizens (Greenwald, 2014). The scope of this surveillance operation greatly angered governments and heads of state of US allies, particularly the French government, that subsequently summoned the U.S. ambassador for an

explanation, urging renewed talks on the protection of personal data, and demanding pledges that the surveillance would cease (Gellman & Poitras, 2013).

Although it may be true that all nations gather information and intelligence, it is not true that they have the same technological capacity for doing so. The power, scope, and breadth of US intelligence gathering through electronic surveillance supersede that of most, if not all, other nations. From this vantage point, one is looking at not quantitative, but qualitative differences in surveillance systems with significantly different implications and impacts on democracy, transparency, the rule of law, and human rights. The difference in technological capacity between the US and other countries, with the exception of perhaps China, alters the conditions and breadth of surveillance capabilities, rendering the US system more totalizing, and as some have argued, more totalitarian (Boghosian, 2013).

The perceived tendency of the US surveillance system to evolve in the direction of totalitarianism is reflected not only in conducting surveillance on what are deemed enemy states and enemy targets, but more importantly on what are deemed friendly and even closely allied states (Boghosian, 2013; Frontline, 2014; Greenwald, 2014). For example, when it was revealed that a US surveillance operation known as Flat Liquid secretly accessed Mexico's presidential domain and eavesdropped on the communications of former Mexican President Felipe Calderon and his Cabinet, it led the Mexican government to issue a diplomatic rebuke towards the US (Chumley, 2013).

US surveillance criticism did not end with Mexico. In protest, Brazilian President Dilma Rousseff canceled a state visit to Washington, DC, and condemned the US at the United Nations General Assembly, when it was disclosed that the US had electronically

intruded into Brazil's communications systems (Lynch, 2013). Following Snowden's revelations, it was concluded that the NSA had hacked into Brazil's networks of state-run oil company Petrobras, intercepted Rousseff's communications, and was monitoring data of billions of emails and telephone calls across Brazil (Lynch).

US surveillance came to a highpoint of diplomatic awkwardness when, in July 2014, it was revealed, again through Snowden, that the NSA was intercepting German Chancellor Angela Merkel's cell phone communications. According to a report by *Der Spiegel*, the NSA in cooperation with the UK Communications Headquarters, had launched a program coded Five Eyes, that intended to map the entire Internet, and had infiltrated the networks of Germany's Deutsche Telekom Netcologn (Frontline, 2014).

The news about the NSA spying on Germany's Chancellor and Germany's communication networks was met with hostility by German public opinion. Especially in light of Germany's unsettling memories of government surveillance by the Gestapo during the Nazi era, and later by the Stasi police in East Germany during the Communist era. In response, the German government annulled a Cold War-era agreement that allowed the US and Britain to request German authorities to conduct surveillance operations within the country to protect their troops stationed there (Eddy, 2015).

It appeared that Germans were made more uneasy when they were invited to join the American led, so called *Five Eyes*, a treaty-based alliance between the intelligence services of the US, Australia, Canada, New Zealand, and the UK for the purpose of cooperation in global intelligence gathering (Passenheim, 2013). The premise in joining was that in avoiding surveillance by the members of the Five Eyes organization,

Germany had to agree in helping spy on the rest of the world and share the information that was collected when asked (Passenheim).

Already in 1998, following the publication of a book by New Zealand journalist Nicky Hager (1996) entitled *Secret Power: New Zealand's role in the International Spy Network*, the European Parliament issued a report titled "An Appraisal of the Technology of Political Control." The report stated that, within Europe, all email, telephone, and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland via the strategic hub of London then by Satellite to Fort Meade in Maryland via the crucial hub Menwith Hill in the North Yorkshire Moors of the UK (European Parliament, 2014). The European Parliament subsequently called for a resolution that, had it passed, would have required dismantling Five Eyes programs such as ECHELON—a system of international surveillance mechanisms with the capacity to intercept, retrieve, and store nearly all forms of electronic information (Frontline, 2014; Greenwald, 2014). These initiatives were ultimately hindered, without reaching conclusion.

Nationalism, War, and the Legitimization of Surveillance

It appears that in the aftermath of the 9/11 al Qaeda attacks on US soil, the historical confluence of aggressive nationalism and the evolution of technology in the sphere of electronic surveillance, not only marginalized and postponed any serious democracy-driven inquiries into the legitimacy and extent of surveillance, but it has created the conditions for removing all limits to expanding the scope of state surveillance (Boghosian, 2013; Givens, 2014).

In light of the growing powers of state surveillance, the big shock for American citizens came in 2013, when the media disclosed domestic surveillance practices under titles such as “Confirmed: The NSA is Spying on Millions of Americans” (Cohn, 2013), “NSA collecting phone records of millions of Verizon customers daily” (Greenwald, 2013) and “Spying on millions of Americans in the ‘United States of Secrets” (Frontline, 2014), among others. According to *The Guardian*, the NSA was conducting sweeping, un-targeted, domestic surveillance on millions of Americans. It revealed that:

> The National Security Agency is currently collecting the telephone records of millions of US customers of Verizon, one of America’s largest telecoms providers, under a top-secret court order issued in April.
>
> The order, a copy of which has been obtained by the Guardian, requires Verizon on an “ongoing, daily basis,” to give the NSA information on all telephone calls in its systems, both within the US and between the US and other countries (Greenwald, June 6, 2013, para.1 & 2)

The government order was issued in accordance with Section 215 of the PATRIOT Act. The assumption was that domestic surveillance went on for years and extends to other American telecommunications companies (Greenwald, 2013). Here again, one can see how current surveillance practices disclose a seamless digital networking, linking government digital systems and private sector digital systems, simply by opening a portal, following a court order.

The intensification of domestic surveillance fits in the framework of the US wars against terrorism in combination with reactive retaliations to America’s wars on

terrorism. Surveillance targets not only those under suspicion of being foreign terrorists, but also homegrown terrorists. Since the commencement of the wars in Afghanistan and Iraq, America has experienced a number of domestic terrorist attacks, launched by US citizens (Frontline, 2014). The fear of domestic terrorism escalated with the rise of the violent Islamic State of Iraq and Syria (ISIS) in the fall of 2014. Acts of domestic terrorism were perpetrated not only by American citizens with ties to the Islamic militant organization abroad, but also by US citizens who became radicalized, perhaps through the internet, who acted alone (Frontline).

Under the conditions that protracted warfare creates, unimpeded domestic surveillance acquires its justification and rationale of national necessity—the very argument that pro-surveillance advocates put forward. However, such an argument cannot be easily dismissed by the anti-surveillance advocates, without a clear understanding and realistic critique of the nature of warfare and how it erodes democracy domestically as well. It is under the tragic conditions of violence and protracted warfare that, after the January 2015 terrorist attacks in Paris relating to cartoonist Charlie Hebdo and then in November resulting in the deaths of 130 people and hundreds injured, both the US and the UK demanded that private internet service providers loosen encryptions to enable government to both conduct sweeping surveillance over their clients and to offset use of encrypted communications by terrorists (Jaffe & Zezima, 2015).

Under conditions of war, the nationalist narrative tends to spring back to the historical forefront. It also shapes the state's policies, and political culture, toward the most extreme utilization of technological power. In this context, rather than being democratically conditioned and managed, technological power becomes a weapon of the

state that is used with the primary intent of defeating the nation's enemies, in the name of national security (Anastasiou, 2011).

Once this power becomes institutionalized by the state, it becomes progressively regarded as concurrent with national survival and national security (Frontline, 2014). Within this context, emerges the notion of American exceptionalism, which is at the heart of the American nationalist narrative (McCartney, 2004). This notion defines the supreme power of America as a benevolent and morally auspicious force. In this way American exceptionalism justifies the full and unrestrained use of technological power in both the state's foreign and domestic policy approaches (McCartney). Thus, the state, within the combination of nationalism, warfare, and technological power, appears to be driven by the realist theory of international relations, where raw power is what matters.

In addition, nationalism creates a general culture of high tolerance for the use of lethal force and the engagement in war (Howard, 1994). It also vastly increases the power of the state rendering it legitimate in the eyes of the citizens. Self-proclaimed nationalist, Blankley (2009), asserted that in nationalism, the status and power of the nation state is above the value of democracy and human rights. Moreover, the nationalist fails to acknowledge that warfare is always regressive to democracy (Anastasiou 2008; 2011). According to Anastasiou (2008) this constitutes one of the largest blind spots of nationalist thinking because in its narrative it sees warfare as a legitimate instrument of the nation, by which "the good" of the nation can be pursued, and through which the nation's democratic regime and values can be defended and protected. What can be observed historically, however, is that the preservation of democratic values is nearly impossible to uphold once the nation decides to resort to violent conflict. Even prior to

the rise in electronic surveillance, whenever nations engaged in warfare, no matter how much they professed the value of democracy, they inevitably rolled back democratic processes, democratic legislation, democratic rights, and democratic oversight of the state's activities (Anastasiou).

The surveillance phenomenon and its relation to human rights can be likened to the dichotomous regression of democracy in an effort to uphold democratic values under the conditions that warfare and nationalism create. With current technology, however, the relationship appears to be more sophisticated, complex, elusive, and more concealed. This is due to the intangible and abstract nature of the digital world, and its integration into the bureaucratic institutions of both the state and the corporate world of information technology (Castells, 2010; Ellul, 1980).

Here one can ascertain the idea that the interaction between nationalism, warfare and technology in America's response to 9/11 and the decades that followed, played a significant role with regard surveillance and the justification of its expansion. The immediate, and sustained, rise in American nationalism following the 9/11 terrorist's attacks, and its relation to technology, the law, and warfare, has been a significantly neglected element in the surveillance debate. Populist nationalism made public opinion tolerant to surveillance and generally more tolerant to authoritarian executive actions by government agencies and the state (McCartney, 2004). Simultaneously, the sustained nationalism in the post-9/11 era rendered the American citizenry and political leadership more complaisant in regard to exercising any credible and serious measures of democratic oversight of the actions of both government and corporations engaged in the surveillance system of the state.

What is interesting, is that the entire logic of the approaches developed and secured by law for protecting personal data through encryptions is exactly the same as the one used during World War II for maintaining secrecy in strategic communications (Freedman, 1995). It appears that the problems and challenges raised by technological advances in securing the personal data of citizens, as a legitimate pursuit, is structurally similar to the secrecy procedures, through methods of encryption that become prevalent during times of war. This particular revelation, brings to the forefront the largely unaddressed question as to whether there is an affinity between, on the one hand, threats to human rights and democracy posed by the power of technology, and, on the other hand, the conditions that come into play during wartime, particularly in regard to national security.

In this regard, the Bush administration's launching of the "global war on terror" in effect set the stage for the vast expansion of executive state powers, especially in the realm of surveillance, among others (Peterson, 2009). Sweeping criticism of US government failures in being able to foresee and preempt the 9/11 attacks, and the fact that certain laws existed that restricted preemptive actions of the state to advert similar threats, all led to widespread changes aimed at redefining what is legal in regard to the actions of the state in the name of national defense (Byman & Wittes, 2014). In the wake of this restructuring came the mass explosion of resources dedicated to electronic mass surveillance (Frontline, 2014).

The USA PATRIOT Act and the set of laws derived from it are primarily designed to protect the homeland, to preempt attacks similar to 9/11 and any terrorist attacks in general. In doing so however, the USA PATRIOT Act is also designed to

accommodate warfare (USA Patriot Act). In other words, the laws that come into force under war conditions intend, among other things, to render legal, and hence legitimate, the array of actions that, once at war, the state is compelled to take, which under peaceful conditions are generally deemed illegitimate, illegal, and widely unacceptable as undemocratic, harmful to human rights, and even unconstitutional (Anastasiou, 2009; Howard, 1994).

Under conditions of war, the legislation that Congress passes becomes exceedingly ambiguous (Savage, 2013), as it is no longer primarily democratic, but rather enhances and protects the position of the state in resorting to actions that in their essence are undemocratic and erosive to human rights and democratic freedoms (Matiya, 2013). This is not unique to the US, but to any state that resorts to warfare (Anastasiou, 2008). It is nearly universal that warfare always generates a historical process that pulls legislation in an undemocratic direction (Anastasiou). Warfare has a historical pattern of giving rise to legislation that dissociates the rule of law from democracy and human rights. As a result, this pattern often renders the rule of law an excuse of the state in the postponing, suppression and even violation of democracy, in the interest of what is conventionally called emergency measures. However, although the law may introduce provisions for such emergency measures, it does not make them democratic (Givens, 2014). Consequently, some of the checks and balances of government, one of the key principles of democracy, had been eroded by the Bush administration. Under war conditions the law and democracy become divergent and even contradictory elements of governance (Givens).

Givens (2013) evokes a ratchet metaphor to describe the complementary effect of

legislation and regulatory powers to incrementally concentrate power. Givens argues that in the face of terrorism, the US government through the USA PATRIOT Act, has given legal powers to its intelligence agencies that in effect erode the traditional protection of human rights and citizen privacy rights in particular. He acknowledges that the laws that gave the state extended surveillance powers are in essence undemocratic. But more importantly, Givens stresses the difficulty in reversing or repealing undemocratic legislation as long as the threat and fear of terrorism persist, and as long as the country is at war. The dynamic in the direction of undemocratic legislation, he argues, can become so powerful and legitimate in the eyes of political leaders and citizens that undemocratic legislation tends to be normalized and may even become permanent.

One could argue that this historical process of moving the system of governance in an undemocratic direction is not necessarily a choice but a necessity that structurally accompanies the conditions of war. Moreover, it follows the decision to engage in war, as a reasoning of legality that accommodates the extremities of war, to which the state and the government must inevitably resort, and that the populace must inevitably comply. Once a society enters the realm of war, this dynamic is unleashed. For once within the arena of warfare, the freedoms that the democratic process so ardently aspirers to project as its cornerstone, quickly distort into nearly unattainable ambitions. Under conditions of war, and in particular when it comes to the actions that war requires, freedom dissipates. And where freedom is downgraded, so is democracy (Anastasiou, 2011). In the language of human needs theory (Burton, 1993) the basic need for security gradually supersedes the basic need for liberty. These conditions, and the historical dynamic they engender, do

not provide the moral rationale for unimpeded or aggressive surveillance, as the pro-surveillance advocates argue. Rather, they underscore the tragedies of war and the freedom-eroding environments that protracted warfare creates. In addition, what goes largely unnoticed is that national security considerations result in a systematic erosion of democracy and human rights. I would argue that under conditions of protracted warfare, with the heightening of the nationalist narrative, dictating general opinion and policy orientation, it appears that it is always national security that takes precedent over human rights and democracy. With regard to our analysis of the topic, one can now conclude that the phenomenon of surveillance under conditions of protracted conflict creates increasing power asymmetry in the interest of the state, over-against the rights of citizen.

The sustained rise in American nationalism and America's engagement in protracted warfare in the post-9/11 era has not been adequately addressed with regard to its impact on the surveillance issue. The analysis strongly suggests that the rise of nationalism and the protracted wars on terror of the post-9/11 era may have greatly affected the phenomenon of surveillance. In summary, the attacks of 9/11 and the wars that followed, reinforced the pressure and necessity for aggressive surveillance, since the need to avert other terrorist attacks became the primary concern of both governments and citizens. The rise of nationalism that accompanied the attacks created a broad sense of "legitimacy" for the US wars against Islamic militancy. The fear and uncertainty among the citizens has tolerated excessive executive actions by the government, including surveillance. Especially during the Bush administration, the government capitalized and exploited public fear, while targeting critics of surveillance us unpatriotic and dangerous for national security. Under these conditions, the most nationalist political leaders,

endorsing the wars, also felt empowered and justified to support enhanced surveillance, which finally reached unprecedented levels. In this way, the rise of nationalism and the protracted wars against terrorism played a vital role in creating the conditions that made the surveillance phenomenon appear necessary and acceptable. However, neither the advocates nor the critics of state surveillance have taken the impact of nationalism and the wars sufficiently into account.

State Secrecy and Surveillance

Conditions of protracted warfare combined with current technological surveillance abilities, appear to be catalysts for elements of the state structure, entailing national security bodies, becoming increasingly clandestine. Even prior to the emergence of the of the digital revolution, sociologist Max Weber argued that with its rising specialization and complexity, bureaucracy, at its core, while greatly efficient, becomes secretive and non-transparent, curtailing individual freedom as in an iron cage (Gabriel, 2005). With the rise of the digital world and the network society, this tendency toward secrecy in the structure of the state's security apparatus becomes even more acute, including its digital, networked relationship to private sector collaborations. When it comes to state surveillance, the so-called principal of "plausible deniability" tends to become commonplace (Givens, 2014). For example, while it is now known that surveillance programs such as Echelon has long been part of the state's surveillance arsenal, the US government have remained mute regarding its existence (Ward, 2001). Regardless of which party is in power, systematic government denial and/or secrecy regarding its surveillance operations, including surveillance on US citizens, has become

quite routine, with protracted wars and fears of domestic terrorism, providing the credible brunt of the pro-surveillance argument.

Nevertheless, the implications of state secrecy in the erosion of democracy and human rights are equally real and credible. What is more challenging are not only the secretive activities of the state, but also the secretive ways in which the state interprets the pertinent laws regarding surveillance. For example, in May 2011, Democrat Senator Ron Wyden, one of the few voices posing the difficult questions regarding the government's domestic surveillance program, expressed during a debate about reauthorizing Section 215 of the USA PATRIOT Act, that Americans will be stunned and greatly upset when they find out how misleading the act is (Savage, 2013). As only one example of a historical trend, Wyden's warning discloses the challenge of a much bigger picture. Namely, that, in the digital age, under conditions of war embedded in sustained nationalist fervor, the surveillance state tends to exhibit all the features of the so-called 'deep state' (Frontline, 2014). That is, there is the creation of an array of airtight sectors deep inside the state that the democratic process cannot reach or touch; where there is no transparency, no public access or knowledge, no democratic oversight, no clear interpretation of the law, no civil society engagement in limiting or delineating state power (Cohn, 2013). This is also expressed in the 2014 documentary titled *United States of Secrets*, a Frontline documentary aired by the Public Broadcasting Service (PBS) disclosing the evolution of US secrecy and America's domestic surveillance program (Frontline). In this piece, Barton Gellman uses the analogy of a 'one-way mirror' that has been created, where the government can see what everyone else is doing, but no one can see what the government is doing (Frontline). In addition, Gellman concludes the

documentary with the concerning dilemma that we cannot truly hold our government accountable because we are not entirely sure of the actions and legislative measures that are being carried out.

In light of this analysis, the prevalent tension between national security considerations and human rights, including human security, appears in a rather different light than in the manner political leaders, academics and journalists pose the issue. When it comes to attempted resolutions and the way forward in addressing the polarization between national security and citizen rights much remains unanswered and vague. As a result, even when they are sensitive and aware that the power of state surveillance, in cooperation with sector corporations, entails infringement on citizen rights, political leaders with positions in government have extreme difficulty addressing the essence of the surveillance issue and the challenges it poses to democracy. The position they generally assume is to simply say that one needs to strike a balance between national security considerations and human rights, including the right to privacy (Etzioni, 2015). This has been the approach of President Obama, Cameron of the UK, Abbot of Australia, Harper of Canada, and generally of most European states and governments, as well as that of like-minded academics and journalists. Paradoxically, while in fierce opposition to US actions, the German Foreign Minister Guido Westerwelle articulated exactly the same position when he stated: “We know there are security interests, but it is about finding the right balance between security interests and freedom rights” (Otto, para. 31, 2013).

What is often neglected in the balancing argument are the questions as to what this balance would look like and what structure it would assume, given the now institutionalized and global reach of surveillance technology. This attempt for balance

would be particularly interesting to see manifested in the context of the on-going and ever broadening conflict between the ongoing military engagement of US-led western powers in Muslim countries and the metastasizing Jihadi militant organizations around the world. Within the framework of the dynamic interactivity between these elements for over a decade, the relationship between national security and human rights, including citizen rights to privacy, has decisively shifted so far in the direction of national security that the hitherto relationship and attempted balance between the two, characteristic of previous eras, has been decisively and structurally broken. In their work *Reforming the NSA*, Byman and Wittes (2014), are among the very few that identify the structural disintegration of the relationship between national security and human rights. And they do so even as they defend the NSA. In their words:

> The real problem that Snowden's revelations brought to light was not a government agency run amok: the NSA never meaningfully exceeded the writ given to it by the White House, Congress, and the courts, at least not intentionally. Rather, those revelations highlighted a basic conflict between two things that U.S. citizens and their government demand from their intelligence agencies: a high, if not perfect, level of security, on the one hand, and strict privacy protections, accountability, and transparency, on the other. Those imperatives were never easy to reconcile and are even harder to resolve today. Indeed, Snowden's revelations demonstrated how the implicit bargain that has governed the U.S intelligence community since the 1970s has broken down (Byman and Wittes, p.128).

The urgent call to balance national security with human rights concerns has not been adequately responded to. In fact, one could conclude that the current surveillance

situation has moved beyond the capacity of balancing security and human rights, because the two elements have moved so divergently that there is no longer a structural relationship between them, in terms of which to attempt a balance. As Byman and Wittes (2014) argue, the functionality of the two working in conjunction with one another appears nearly impossible due to the increasingly polarized dynamic.

The human need for security and the human need for liberty, especially at the citizen level have become dissociated from one another. The consistent and integrated relationship that basic human needs have to each other, according to Human Needs theory, becomes fractured (Byman & Wittes, 2014). Under conditions of protracted wars and nationalism, aggressive surveillance disrupts and breaks down the cohesion and interrelationship between human needs. In this case, the human need for security and the human need for liberty become dissociated from one another.

The discussion here brings to the forefront the complex nature and overlapping structural and contextual factors that influence the surveillance conflict. The conflict analysis addressing the interconnectedness of the psychological impacts of crisis and warfare, and the societal effects of nationalist fervor and rapid technological advancements provides a unique and more overarching perspective on the debate that, illuminates and clarifies the issues.

Chapter 6: Implications and Directions for Further Research

In light of the foregoing, one could propose that the idea that "Big Brother is watching," as presented in George Orwell's fictional work *1984*, has become all too real, and prompts questions as to where the boundaries are, or should be, in regard to state surveillance, leaving many wondering whether there is still such a thing as individual privacy. Revelations of diplomatic espionage, the indisputable partnerships between private and government sectors, and the exponential growth of data storage and state surveillance in the post-9/11 era, has provoked extensive alarm in how the misuse of such power, in the name of national security, may very well be standing in opposition to the democratic values that national security systems are allegedly trying to protect. In essence, the complexities and controversies deriving from post-9/11 surveillance have left the relationship between national security and human rights in a state of ambiguity.

Based on academic literature, media coverage, positions of political leaders and citizens, the dominant debates around the issue of government surveillance revolve around two principal perspectives, which appear to be in direct conflict and opposition to each other. One perspective argues that in a post-9/11 world, mass government surveillance is imperative for national security and the protection of citizens, including the protection of the country's democracy (Allen, 2008; Blankley, 2009; Toxen 2014). The other perspective argues that mass surveillance is not only unnecessary and ineffective but it grossly violates human rights and erodes democracy (Boghosian, 2013; Etzioni, 2013; Greenwald, 2014). These are the dominant competing perspectives on the issue, with respect to which less mainstream and more nuanced perspectives have been formulated.

Numerous amounts and various types of literature have attempted to adequately articulate this polarizing topic. Although both sides of the debate often offer valuable information and perspectives with regard to the issue at hand, there appears to be neglect of contextual issues which impact the vitality of the conflict itself such as how conditions of conflict and protracted warfare, and the accompanying nationalist narrative, may affect resolution.

The current widespread controversies associated with national security concerns, the exposures of metadata storage, diplomatic espionage, corporate-government partnerships, and mass surveillance comprise issues that need to be addressed within a conflict resolution and peace and conflict studies framework—an approach that, as of yet, has not been pursued.

In light of the above, it is legitimate to ask whether or not the use government surveillance, in the interest of national security, to protect the homeland and American citizens under conditions of protracted conflict, is essentially and practically compatible with the practice, values and regime of democracy and human rights, as professed by America.

Implications

My analysis has attempted to disclose the historical and political conditions under which the phenomenon of vastly expanded state surveillance occurs and is sustained. The rise of American nationalism in the aftermath of 9/11, the protracted US engagement in multiple wars in conjunction with terrorism, and the evolving technological powers of the digital world have merged into a singular confluent, dynamic pattern that is driving America, as well as some of its close allies, into increasingly undemocratic territory. I

would argue that unless the confluence of these conditions is deconstructed and gradually and persistently reconstructed, democracy and human rights will be perpetually on the losing side, while national security considerations, and the accompanying nationalist mindset, will perpetually pose reasons for why national security should supersede human rights and human security with regard to the integrity and privacy of citizens, domestically and globally.

It is this historical confluence and integration of nationalism, war, and technological power that both the pro-surveillance and the anti-surveillance advocates miss in their respective approaches to the challenges at hand. The nearly universal nationalism, that conditions and drives the thinking of the pro-surveillance advocates continually tends to transpose the undemocratic, distorted, and abnormal immediate conditions created by protracted warfare into perpetual norms for the governance of society.

With regard to the pro-surveillance supporters, it appears that many of them assume that war is normal and a perpetual condition in the nature of the state. As a result, any undemocratic actions or legislation that comes into force under the constraining and suffering conditions of war is viewed as unproblematic and permanent. I would argue that the research also suggests that the general perspective of pro-surveillance supporters is one that considers such actions by the state as necessary for the protection of the nation's democracy. Similarly, it would appear that the contingencies that deriving from war are interpreted by pro-surveillance advocates as normal, natural, and necessary. As a result, all the undemocratic laws, secretive institutions, and covert power structures that come from, and are extrapolated from the conditions and abnormalities that wars inevitably

create, are viewed as acceptable and permanent (Givens, 2013). It is here, that one sees that familiar, yet sadly unattended pattern of nationalist thinking, where the raw power and status of the nation is the primary order of the state and society (McCartney, 2004), simultaneously superseding and demoting democracy and human rights as a mere appendage of the nation's regime (Matiya, 2013), often expendable in the name of the nation and in the name of nationalistic understanding of national security.

The anti-surveillance advocates, on the other hand, have an equal deficiency in their approach, but for different reasons. I would argue, that one of the most significant deficiencies of the pro-democracy and human rights advocates, is that they assume the nation can be engaged in protracted wars while simultaneously prioritizing and maintaining intact a transparent, domestic regime of democracy, that continues to uphold the rights of citizens. This approach appears to be yet another way of normalizing warfare and neglecting to realize the pressures and social climate that accompany war and violent conflict. More specifically, especially through the presumption of the "just war" doctrine, there is an evasion of the critical and regressive structural impact that warfare has on democracy. It is within this context, that the nationalist narrative that legitimizes war as normal, albeit under certain conditions, creeps into the framework of this category of anti-surveillance advocates. Only it does so in a more subtle way. Sadly, what the anti-surveillance advocates essentially miss is the elephant in room, which is the nature of warfare and its impact on the state and the governance of society. In this configuration of thought, this type of anti-surveillance advocacy fails to see that it is historically impossible to engage in protracted warfare without increasingly and systemically

curtailing, contracting and even violating democracy and human rights domestically and abroad.

The second category of pro-democracy and anti-surveillance advocates concerns those who are not only anti-surveillance, but who are also critical of America's wars. The deficiency in their approach lies in that they see two wrongs that they oppose, namely America's wars and America's excess in domestic and foreign surveillance, but fail to see the intimate structural relationship between warfare and aggressive surveillance. Nor do they see that because of this structural association that erodes democratic safeguards, the state is also compelled to resort to the unimpeded and optimum use of technological power in totalizing its scope on surveillance. In addition, they do not see that the prevalence of nationalism under war conditions orients the state, as well as mainstream public opinion, toward acquiescence and complacency with regard to institutionalized massive surveillance efforts at home and abroad. There is no critique of the structural confluence of war-endorsing nationalism, surveillance, and the sheer and unimpeded use of technological power that tends to always crystalize under war conditions. As a result, the pro-surveillance supporters, who tend to be more overtly nationalistic, easily dismiss the anti-surveillance advocates as being unpatriotic rejectionists—which, by default, leaves the issue of nationalism untouched, allowing it a more free and unobstructed reign.

The crucial issue underlining the phenomenon at hand is not about whether the pro-surveillance supporters or anti-surveillance advocates are right or wrong. Each side possesses a certain level of credibility to its arguments. Rather, the essential issue is that perpetual warfare, accepted by the nationalist world and life-view, gives rise to unresolvable moral dilemmas and structural polarizations in the political culture and

institutions of the state and society, setting in conflicts between security and freedom; national security and citizen security; safety and democracy; national power and citizen power; state sovereignty and citizen sovereignty.

Within this context, and drawing upon human needs theory, it may be virtually impossible to protect both the human need for security and the need for liberty under conflict conditions. The more a country becomes immersed in warfare the more challenging meeting these human needs becomes. In fact, they become structurally opposed to one another. The critical question from the perspective of peace and conflict studies is whether the need for liberty and the need for security can ever be reconciled under conditions of protracted warfare and the nationalism that accompanies it. Based on the present analysis, the answer would be "No." By implication, only when rival groups deescalate violent conflict and start moving in the direction of some kind of resolution and eventually peace, will the need for human security and human liberty be aligned.

In light of this reality, under precarious historical conditions, if and when surveillance is needed to address immediate and unpredictable threats, it is of vital importance not only to strictly streamline such process, but more importantly for government and citizens to premise the phenomenon of massive surveillance under the qualifier "undemocratic emergency measures," thus calling it by its true nature as opposed to identifying it, as nationalists tend to do, as a mere instrument that allegedly protects society and democracy. Similarly, all excessive executive powers, any extra-constitutional measures, secretive actions, as well as regressive legislation that pertains to crisis conditions, especially protracted warfare, should be identified as deviations from

democracy and human rights, and even as directly anti-democratic and directly anti-human rights in nature and orientation.

The immediacies and contingencies that wars and war-related threats create must never be confused with the more on-going, long-term, and permanent normativity of democracy and human rights that democratic regimes profess to seek and maintain. Between the short-term undemocratic emergency measures and the longer term return to, and reinforcement of, democracy it is also crucial for America's foreign policy framework, and that of the west in general, to address decisively and programmatically the long-term causes of terrorism and how to defuse them.

Framing the matter in these ways, underscores the fundamental acknowledgement that, in their essence, the measures pertaining to phenomena such as surveillance are temporary, undesirable, and contrary to the appropriate norms of democratic governance. Furthermore, it underscores the historical fact that, despite nationalist rhetoric to the contrary, when nations go to war their democracies undergo regression and erosion, while governments assume excessive powers, often by popular consent, due to fear rather than civil responsibility. This brings to the forefront one of the most significant and largely neglected aspects of democracy. Namely, that unless a nation, and in this case America, makes peace and peace-building, through peaceful means, an integral part of its domestic and foreign policy framework, and strives toward peace as the normative, national security and national interest objective, issues such as surveillance and other incursions against human rights and democracy cannot be effectively addressed, either in the short or in the long run.

With the utilization of both government and civil society, a path may be charted so that as the nation seeks to move out of and beyond war, the undemocratic emergency security measures, institutions and practices could be systematically reviewed, dismantled, constrained, and systematically placed under a democratic regime of transparency and oversight. It is only when the nation seeks strategies toward peace, and moves in that direction, that democracy may be genuinely secured, and where a regime of human rights can prevail as the primary order of the state and society. With this said, if we the people, citizens and officials alike, are able to cease pointing fingers at one another, and could build upon the awareness of the interrelated, underlying, often unattended and neglected factors beneath the surveillance issue, and step outside of the realist and nationalistic mindset that legitimizes and normalizes warfare, the human need for both security and freedom may have the long overdue opportunity of rising together in unison.

Through the introduction of the factor of technology, the analysis strongly suggests that while the growing power of technology in the digital age has grown enormously, thus increasing the capacity for surveillance, it has not been sufficiently addressed in the mainstream debate on the issue. As the digital age has created a global electronic network, on which surveillance depends, technology and its impact need to be assessed critically, as it is integral to and contextualizes the surveillance phenomenon.

Through the introduction of the new factor of rising nationalism and protracted warfare in the post-9/11 era, the analysis has suggested the impact this factor has had on the phenomenon of surveillance. Since the need to avert other terrorist attacks became the primary concern of both government and citizens post-9/11, there were considerable

pressures and justifications for aggressive surveillance. Simultaneously, the rise of nationalism that accompanied and supported the wars created a broad sense of "legitimacy" for the US wars against Islamic militancy, which, due to fear and uncertainty, led to a tolerance for excessive executive actions by the government, including expanded surveillance.

Finally, it ought to be noted that human needs theory (Burton, 1993) identifies the problem as a polarization between the basic human need for security and the human need for liberty, and eventually as a severing of the relationship between the two basic human needs. In contrast to the condition of war, the implication here is that only under conditions of peace may the human need for security and the human need for liberty become harmonious and mutually reinforcing.

In light of this inquiry, the following chart offers an overview of the various levels of integration of surveillance, technology and nationalism, and their dynamic interactions in polarizing the need for security and the need for liberty, and in shifting power from the citizens to the state and corporations. The chart reflects the various levels of data and higher-level categories that have been generated from the analysis, in line with the methodology of grounded theory. Figure 8, beginning on the following page and composed of three diagrams, provides the basis for a more comprehensive and integrated conflict theory of surveillance. The figure is first presented in its entirety to better illustrate the flow and interconnected dynamics of the conflict, and then broken down into sections that are more legible.

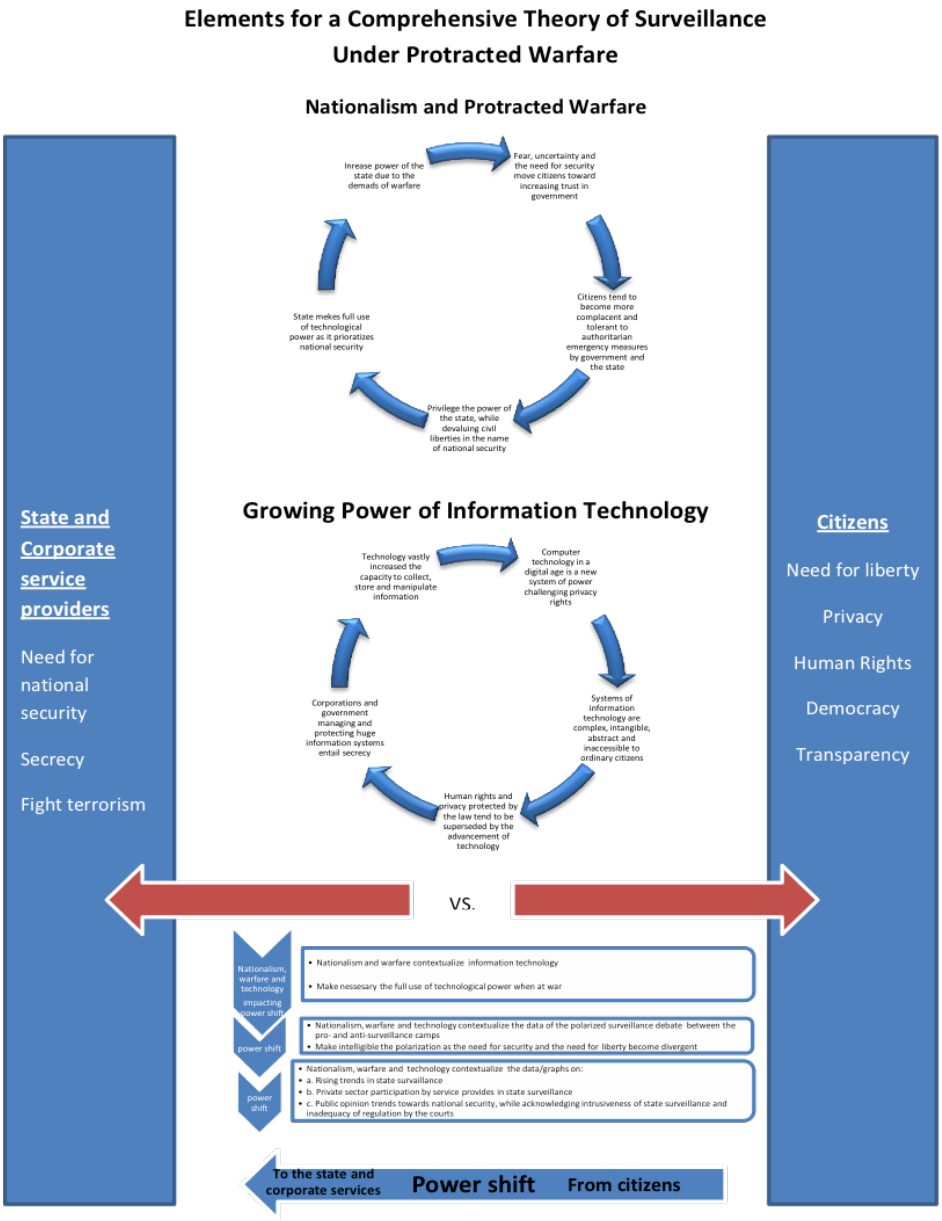


Figure 8: Elements for a Comprehensive Theory of Surveillance under Protracted Warfare

Figure 8a: Nationalism under Protracted Warfare

Elements for a Comprehensive Theory of Surveillance under Protracted Warfare

Nationalism under Protracted Warfare

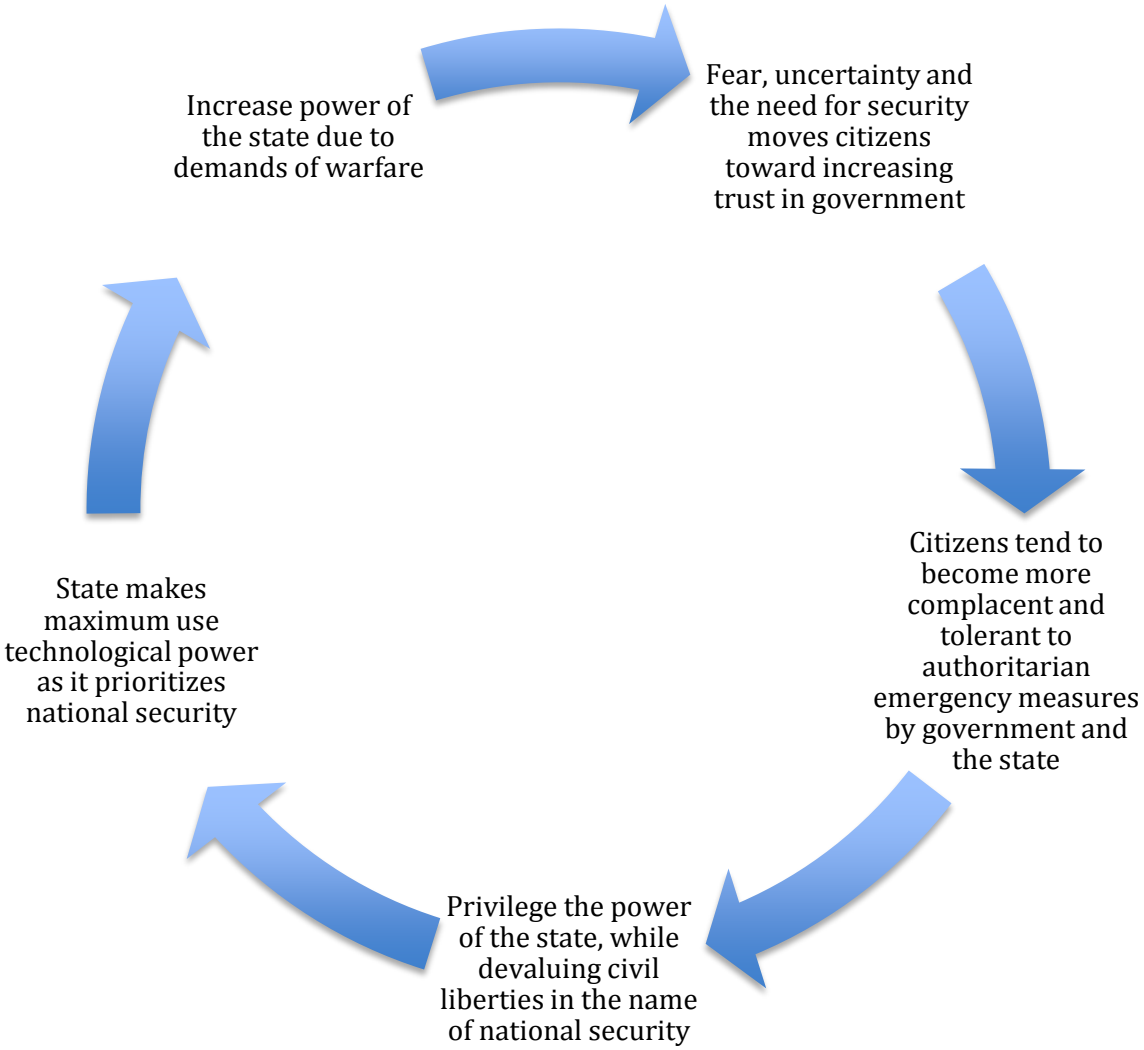


Figure 8b: Growing Power of Information Technology and the Impact on Human Rights

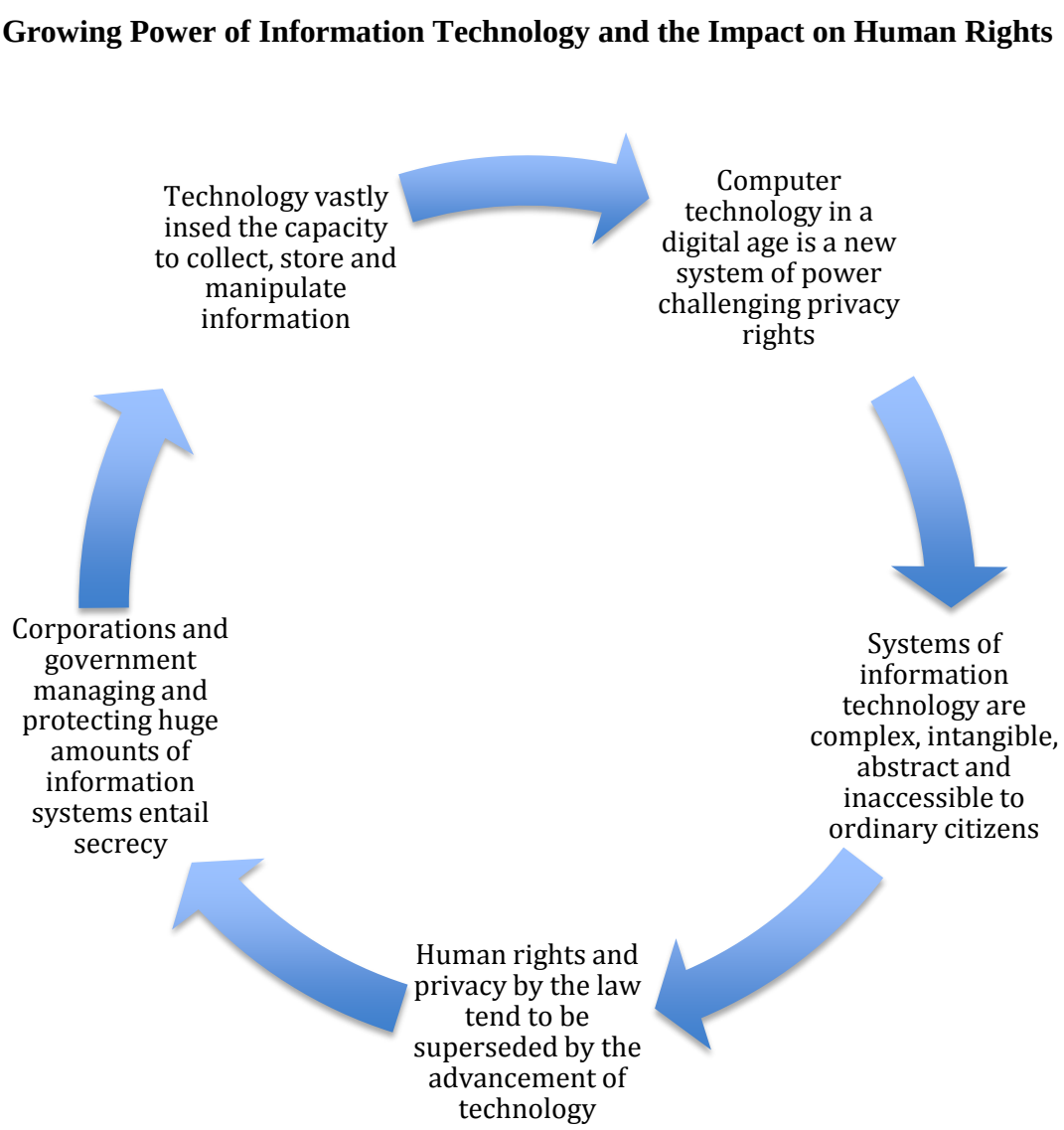
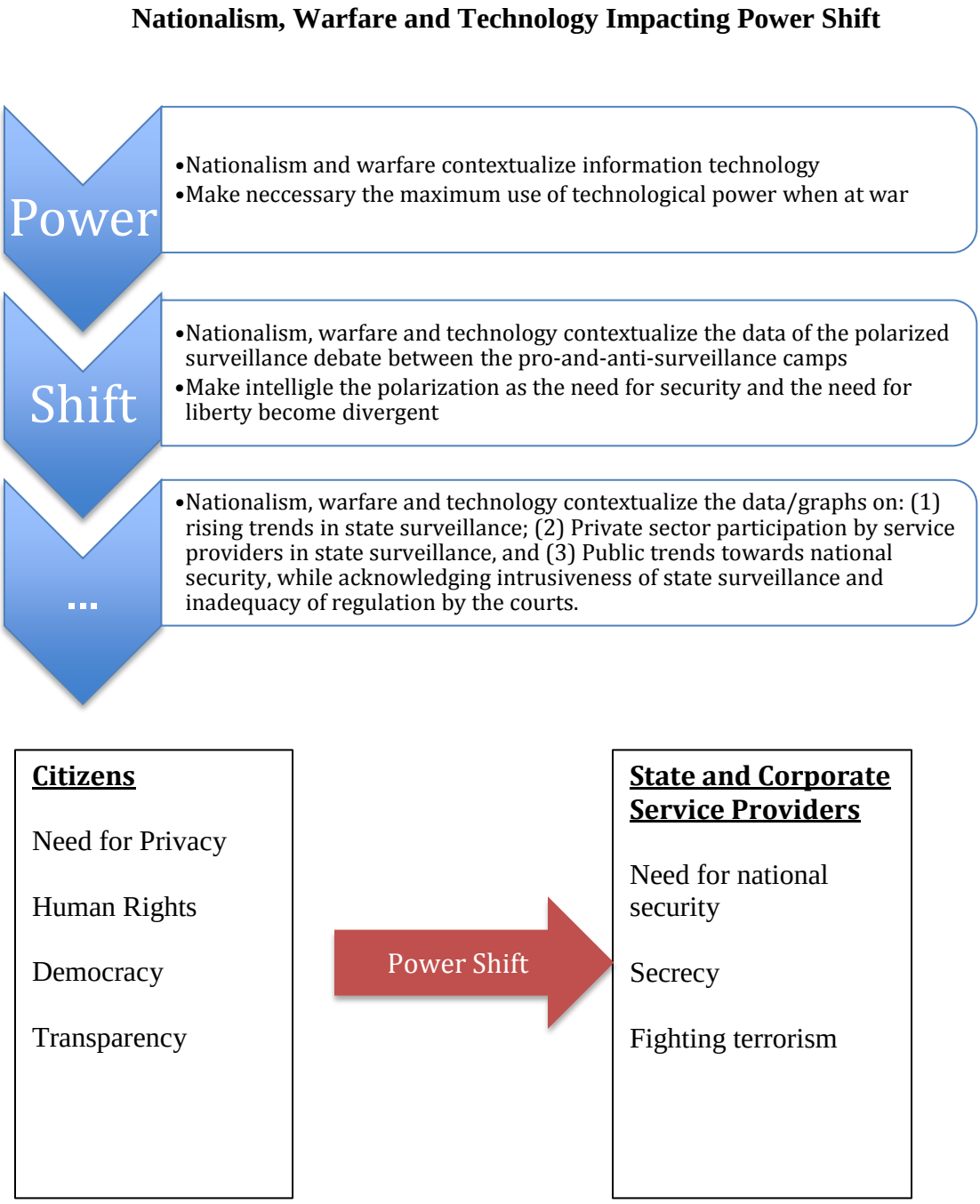


Figure 8c: Nationalism, Warfare and Technology Impacting Power Shift



Limitations

As with most research endeavors, a relative amount of limitation is to be expected. This study sought to observe and analyze a particular issue with the hopes of offering more comprehensive and accurate conclusions than perhaps its predecessors. For this study in particular, one could argue that the most significant limitation pertains to how current and complex the surveillance issue is. Not only is there is a continuous output of both peer-reviewed and mainstream literature on the topic, but the conflict itself continues to evolve due to the enfolding of the various dynamics that influence it. For example, with the sustained influence of ISIS and violent Jihadist movements, coupled with acts of terror both domestic and abroad, one could argue that the surveillance phenomenon is becoming more elusive and intangible.

Moreover, a significant aspect of state surveillance involves secrecy, which poses limitations for the researcher due to the lack of access to relevant data. In addition, the number of factors associated with researching surveillance has a very broad range, with complex interconnections. Another limitation is the speed by which the surveillance is currently changing. These changes are due technological developments, the political process, and competing ideologies surrounding the issue.

In addition, one could argue that the qualitative research method possesses certain limitations, especially with regard to the employment of narrative research. Although there are many benefits to narrative research, the researcher must be aware that the information under analyses is subject to one's personal experience and/or opinion. Narratives are typically studied more through their effects and consequences. For example, nationalism as a narrative is generally researched through its impact on policy,

behavior, and action. A scientist studying stresses on a bridge can conduct his or her research with mathematical accuracy. By contrast a researcher studying the impact of nationalism on surveillance is not something that he or she can do with the same approach or mathematical precision because it must be inferred rather than directly observed. This is due to the fact that the subject matter belongs to the human world and is much more complex.

Further Research

The topic analyzed in the present study is already complex and challenging enough that further studies could enrich understanding. An area that would benefit from additional integration is the role of technology in relation to democracy and human rights. It is widely acknowledged that the growth of technology opens up numerous opportunities for progress in a range of spheres from industry, communication, economic development, etc. However, more research is needed to assess how technological development may pose an obstruction to democracy and human rights. Another area for further research would explore how to maintain a viable balance between the need for liberty and the need for security under conditions of crisis. More specifically, further research may be needed in how to chart and secure a pathway that overcomes the Ratchet Effect (Givens, 2013) and provides a roadmap back to democratic processes and legislation of human rights that may have been compromised under crisis conditions. Further research may also include how political leaders and citizens may preempt the pitfalls of nationalism and its tendency to normalize warfare that in turn compromises democracy.

References

Abdo, A. (2013, June). ACLU to Court: Government Spying Invades Privacy of Each and Every American. Retrieved June 17, 2015, from https://www.aclu.org/blog/aclu-court-government-spying-invades-privacy-each-and-every-american

American Civil Liberties Union. (n.d.). Retrieved May 30, 2016, from https://www.aclu.org/

Allen, J. (2008). Expanding Law Enforcement Discretion: How the Supreme Court's Post-September 11th Decisions Reflect Necessary Prudence. *Suffolk University Law Review, 41*(3).

Alter, P. (1994*). Nationalism*. London: Edward Arnold, Hodder Headline Group.

Anastasiou, H. (2011). A Conflict Analysis and Peace Studies Perspective on American Nationalism and US Foreign Policy. Paper presented at the *Annual Conference of the International Studies Association,* Montreal, Canada, March 16, 2011.

Anastasiou, H. (with Broome, B. J.) (2010). "Nationalism." In Ronald L. Jackson II (Ed.) *Encyclopedia of Identity*. Volumes I & II. Sage.

Anastasiou, H. (2008). "Encountering Nationalism: The Contribution of Peace Studies and Conflict Resolution." In Dennis J. D. Sandole, Sean Byrne, Ingrid Sandole-Staroste, Jessica Senehi (Eds.) *Handbook of Conflict Analysis and Resolution.* New York: Routledge.

Anastasiou, H. (2007). "Securing Human Rights Through War and Peace: From Paradox to Opportunity." In Gail M. Presbey (Ed.) *Philosophical Perspectives on the War on Terrorism*. The Philosophy of Peace series. Amsterdam: Rodopi Press

Apfo, Pfo, Cecore, & Fewer. *Conflict-sensitive Approaches to Development, Humanitarian Assistance and Peacebuilding: Tools for Peace and Conflict Impact Assessment*. London: International Alert, 2004. Print.

Bacevich, A.J. (2009). *The Limits of Power: The End of American Exceptionalism.* Metropolitan Books/Holt Paperbacks.

Bamford, J. (2008). *The shadow factory: The ultra-secret NSA from 9/11 to the eavesdropping on America*. New York: Doubleday.

Barash, D., & Webel, C. (2014). *Peace and Conflict Studies* (Third ed.). SAGE Publications.

Belvedere, M. (2014, June 5). Snowden a 'traitor': Andreessen. Retrieved from http://www.cnbc.com/id/101733893

Blankley, T. (2009). *American grit: What it will take to survive and win in the 21st century*. Ashland, OR: Blackstone Audio.

Boghosian, H. (2013). *Spying on democracy: Government surveillance, corporate power, and public resistance*.

Byman, D., & Wittes, B. (2014). Reforming the NSA. *Foreign Affairs*, *93*(3), 127-138.

Burton, J. (1993). *Conflict: Human Needs Theory.* New York: Palgrave Macmillan.

Cassidy, J. (2013) Why Edward Snowden Is a Hero. *The New Yorker*. Retrieved from http://www.newyorker.com/rational-irrationality/why-edward-snowden-is-a-hero

Castells, M. (2010). *The rise of the network society* (2nd ed.). Malden, Mass.: Blackwell.

Clark, M. P. (2013, June 10). Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic. Retrieved April 30, 2015, from http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/

Chumley, C. K. (2013, October 21). Mexico outraged at U.S. surveillance of ally Felipe Calderon. Retrieved May 30, 2016, from http://www.washingtontimes.com/news/2013/oct/21/mexico-outraged-us-surveillance-felipe-calderon/

Cohn, C. (2013, June 7). In Response to the NSA, We Need A New Church Committee and We Need It Now. Retrieved from https://www.eff.org/deeplinks/2013/06/response-nsa-we-need-new-church-commission-and-we-need-it-now

Cook, J. (2012, June 02). Gov't Financial Surveillance Hit All-Time High in 2011, While Surveillance of Terrorist Activity Dropped. Retrieved April 30, 2015, from http://irregulartimes.com/2012/06/02/govt-financial-surveillance-hit-all-time-high-in-2011-while-surveillance-of-terrorist-activity-dropped/

Dann, C. (2014, May 28). Kerry: Snowden a "Coward" and "Traitor." *NBC News.* Retrieved from http://www.nbcnews.com/politics/first-read/kerry-snowden-coward-traitor-n116366

Davies, C. (2015, March 10). NSA sued over surveillance by Wikimedia & more.

Retrieved May 29, 2016, from http://www.slashgear.com/nsa-sued-over-surveillance-by-wikimedia-more-10373066/

Debenedetti, G. (2013, June 7). Factbox: History of mass surveillance in the United States. Retrieved April 11, 2015, from http://www.reuters.com/article/2013/06/07/us-usa-security-records-factbox-idUSBRE95617O20130607

Dost, M. (2013, July 25). Perceptions of Government's Data Collection and Views of Program. Retrieved April 30, 2015, from http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/4-perceptions-of-governments-data-collection-and-views-of-program/

Eddy, M. (2015). File Is Said to Confirm N.S.A. Spied on Merkel. Retrieved March 30, 2016, from http://www.nytimes.com/2015/07/02/world/europe/file-is-said-to-confirm-nsa-spied-on-merkel.html?_r=0

Ellul, J. (1964). *The technological society*. New York: Vintage Books.

Ellul, J. (1980) The Technological System. New York: Continuum Press.

Epatko, L. (2014, January 14). Former Defense Secretary Gates calls NSA leaker Snowden a 'traitor'. *PBS News Hour*. Retrieved from http://www.pbs.org/newshour/rundown/gates-on-snowden/

Etzioni, A. (2015) NSA: National Security vs. Individual Rights. *Intelligence and National. Security*. 30 (1) 100-136. doi :10.1080/02684527.2013.867221

Freeman, E. (1995). When Technology and Privacy Collide. *Information Systems Security*, *11*(4), 62-66. Retrieved from http://www.ittoday.info/AIMS/DSM/82-30-10.pdf

Friedman, G. (2014, April 22). Keeping the NSA in Perspective. Retrieved. *Geopolitical Weekly*. Retrieved form https://www.stratfor.com/weekly/keeping-nsa-perspective

Frontline, (2014, May 13 & May 20). United States of Secrets. Part one and Part two. *OPB.* Retrieved from http://www.pbs.org/wgbh/pages/frontline/united-states-of-secrets/

Gabriel, Y. (2005). Glass Cages and Glass Palaces: Images of Organization in Image-Conscious Times. *Organization*, 9-27.

Gallagher, S. (2013, July 22). JURIST - A Short History of the NSA. . Retrieved from

http://jurist.org/feature/2013/07/nsa-overview-2.php

Gellman, B., & Poitras, L. (2013, June 7). NSA slide explain the Prism data-collection. *Washington Post*. Retrieved from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Givens, A. D. (2013, July 2). "The NSA Surveillance Controversy: How the Ratchet Effect Can Impact Anti-Terrorism Laws." *Harvard National Security Journal*. Retrieved from http://harvardnsj.org/2013/07/the-nsa-surveillance-controversy-how-the-ratchet-effect-can-impact-anti-terrorism-laws/

Grant, G. (2011). *Technology and Empire: Perspectives on North America.* Concord : House of Anansi Press.

Greene, R. (2011, May 9). When is Enough Enough? Government Surveillance Skyrockets in 2010. Retrieved from from https://www.aclu.org/blog/speakeasy/when-enough-enough-government-surveillance-skyrockets-2010

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Metropolitan Books, Henry Holt.

Hager, N. (1996). *Secret power*. Nelson, New Zealand: Craig Potton.

Hakim, P. (2014). The future of US-Brazil relations: Confrontation, cooperation or detachment? *International Affairs, 90*(5), 1161-1180. Retrieved September 30, 2014.

Howard, M. (1994). *War and Nations*. In John Hutchinson & Anthony D. Smith (Eds.), *Nationalism.* (pp. 254-257). Oxford: Oxford University Press.

Immerman, R. (2011). Transforming Analysis: The Intelligence Community's Best Kept Secret. *Intelligence and National Security, 26*(2-3), 159-181. Retrieved September 29, 2014. doi:10.1080/02684527.2011.559138

Ingram, D. (2015, March 10). NSA sued by Wikimedia, rights groups over mass

surveillance - Yahoo News. *Yahoo News.* Retrieved from http://news.yahoo.com/wikipedia-file-lawsuit-challenging-mass-surveillance-nsa-101345997--finance.html

Inkster, N. (2014). The Snowden revelations: Myths and Misapprehensions. *Survival: Global Politics and Strategy*, 56(1), 57-60.

Jaffe, G., & Zezima, K. (2015, January). Obama, Cameron to discuss encryption of online services - *The Washington Post*. Retrieved from http://www.washingtonpost.com/politics/obama-cameron-to-discuss-encryption-of-online-services/2015/01/15/e215effe-9ceb-11e4-96cc-e858eba91ced_story.html

Klein, E. (2013, August 9). Edward Snowden, patriot - The Washington Post. The *Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/wonkblog/wp/2013/08/09/edward-snowden-patriot/

Korab-Karpowicz, W. (2010, July 26). Political Realism in International Relations. Retrieved October 3, 2014.

Kriesberg, L. (1998). *Constructive conflicts: From escalation to resolution*. Lanham, MD: Rowman & Littlefield.

Landau, S. (2010). *Surveillance or security? the risks posed by new wiretapping technologies*. Cambridge, Mass.: MIT Press.

Lee, T. B. (2012, September 27). ACLU forces government to reveal skyrocketing surveillance stats. Retrieved June 16, 2015, from http://arstechnica.com/tech-policy/2012/09/aclu-forces-government-to-reveal-skyrocketing-surveillance-stats/

Lieven, A. (2004a). *America right or wrong: An anatomy of American nationalism*. New York: Oxford University Press.

LoGiurato, B. (2013, June 11). John Boehner: Edward Snowden Is A 'Traitor' – SFGate. SFGate. Retrieved from http://www.sfgate.com/technology/businessinsider/article/JOHN-BOEHNER-Edward-Snowden-Is-A-Traitor-4593261.php

Lomas, N. (2014, November 4). U.K. Spy Agency Chief Goes Public With Anti-Encryption Appeal To U.S. Tech Companies | TechCrunch. *TechCrunch.* Retrieved from http://techcrunch.com/2014/11/04/privacy-not-an-absolute-right/

Lynch. (2013, September 24). Brazil's president condemns NSA spying. Retrieved May

02, 2015, from https://www.washingtonpost.com/world/national-security/brazils-president-condemns-nsa-spying/2013/09/24/fe1f78ee-2525-11e3-b75d-5b7f66349852_story.html

MacAskill, E. (2013, September 9). Yahoo files lawsuit against NSA over user data requests. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests

Matiya, J. (2013). Can there be a human rights approach to international intervention? *Commonwealth Law Bulletin, 39*(1), 105-118. Retrieved September 29, 2014. doi: 10.1080/03050718.2012.755284

McCalmont, L. (2014, February 13). Rand Paul: Take NSA suit to Supreme Court. *Politico.* Retrieved from http://www.politico.com/story/2014/02/rand-paul-nsa-lawsuit-supreme-court-103512.html

McCartney, P. T. (2004). American Nationalism and US Foreign Policy from September 11 to the Iraq War. *Political Science Quarterly*. 119(3), pp. 399-423.

McNiff, C. Timeline: U.S. Spying and Surveillance. *Infoplease.* Retrieved from http://www.infoplease.com/us/government/spying-surveillance-timeline.html

Mears, B. (2014, 12). Government can't hold NSA surveillance data longer – CNNPolitics.com. Retrieved from http://www.cnn.com/2014/03/07/politics/nsa-surveillance-extend/

Melander, E., Bengtsson, M., Ekstedt, J., & Holmberg, B. (2006, January). Manual for Conflict Analysis - Sida. Retrieved May 29, 2016, from http://www.sida.se/contentassets/34a89d3e7cbf497ea58bc24fea7223c5/manual-for-conflict-analysis_1695.pdf

Mumford, L. (1971). *Myth of the Machine: Technics and Human Development.* Mariner Books.

Otto, J. (2013, October 24). NSA Surveillance Angers Our Allies! Retrieved May 30, 2016, from http://conservative-daily.com/2013/10/24/nsa-surveillance-angers-our-allies/

Passenheim, A. (2013, November 22). US lawmakers push for German entrance to Five Eyes spy alliance | Germany | DW.COM | 22.11.2013. Retrieved February 03, 2015, from http://www.dw.com/en/us-lawmakers-push-for-german-entrance-to-five-eyes-spy-alliance/a-17246049

Patton, Marcie J. (Summer, 2006). “Turkey's Tug of War.” *Middle East Report* No. 239,

Dispatches from the War Zones: Iraq and Afghanistan. pp. 42-47. Retrieved from http://www.jstor.org/stable/25164731

Payne, E., & Shah, K. (2013, October 21). Report: U.S. intercepts French phone calls on a 'massive scale' Retrieved May 03, 2015, from http://www.cnn.com/2013/10/21/world/europe/france-nsa-spying/

Peissl, W. (2003). Surveillance and Security: A Dodgy Relationship. *Journal of Contingencies & Crisis Management, 11*(1), 19-24.

Ramsbotham, O., Woodhouse, T., & Miall, H. (2011). *Contemporary conflict resolution: The prevention, management and transformation of deadly conflicts*. Cambridge, UK: Polity.

Rubin, G. (2011). *Freedom and Order: How Democratic Governments Restrict Civil Liberties After Terrorist Attacks—And Why Sometimes They Don't.* Maryland: Lexington Books.

Sanchez, J. (2010, April 30). Your Year in Wiretaps. Retrieved May 29, 2016, from http://www.cato.org/blog/year-wiretaps

Savage, C. (2013). Secret Court Rebuked N.S.A. on Surveillance. *New York Times*. Retrieved from http://www.nytimes.com/2013/08/22/us/2011-ruling-found-an-nsa-program-unconstitutional.html?pagewanted=all&_r=2&

Schneier. (2014, March 3). Schneier on Security. Retrieved May 02, 2015, from https://www.schneier.com/blog/archives/2014/03/metadata_survei.html

Scott, L. (2012). Reflections on the Age of Intelligence. *Intelligence and National Security*, *27*(5), 617-624.

Singel, R. (2008, May 1). Court-Approved Wiretapping Rose 14% in '07. Retrieved April 05, 2015, from https://www.wired.com/2008/05/court-approved/

Smith, C., & Hung, L. (2010). *The Patriot Act issues and controversies*. Springfield, Ill.: Charles C. Thomas Publisher

Sohosian, C. (2009, December 1). 8 Million Reasons for Real Surveillance Oversight. Retrieved from http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html

Surveillance. (2016). Retrieved May 30, 2016, from http://www.pewresearch.org/topics/surveillance/

Toffler, A. (1970). *Future Shock.*New York: Random House.

Toffler, A. (1991). *Powershift: Knowledge, Wealth and Violence at the Edge of the 21st Century.* Batman Books.

Traynor, I. (2013, November 26). NSA surveillance: Europe threatens to freeze US data-sharing arrangements. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing

Toxen, B. (2014, May 1). The NSA and Snowden: Securing the All-Seeing Eye. *Communications*. Retrieved from http://cacm.acm.org/magazines/2014/5/174340-the-nsa-and-snowden/abstract

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

Vicens, A., Gilson, D., & Park, A. (2013, September 11). Timeline: Here's how we got from 9/11 to massive NSA spying on Americans today. Retrieved from http://www.motherjones.com/politics/2013/09/nsa-timeline-surveillance

Ward, M. (2001, May 29). Q&A: What you need to know about Echelon. BBC News: Sci/Tech. Retrieved from http://news.bbc.co.uk/2/hi/sci/tech/1357513.stm

Walpin, G. (2013, August 16). We need NSA surveillance. *National Review*. Retrieved from http://www.nationalreview.com/article/355959/we-need-nsa-surveillance-gerald-walpin

Appendix A

Timeline of US Surveillance

Adapted from: McNiff, C. (n.d.). Timeline: U.S. Spying and Surveillance. Retrieved May 03, 2015, from http://www.infoplease.com/us/government/spying-surveillance-timeline.html

1934	The Federal Communications Act is first law to formally address wiretapping and establishes the Federal Communications Commission (FCC). Under the Act, wiretapping is not illegal, but information gathered may not be disclosed.
1945	The Armed Forces Security Agency (AFSA) begins project SHAMROCK, an intelligence-gathering scheme that collects—without warrants--the international telegrams coming through ITT World International, RCA Global, and Western Union to screen for espionage and Soviet spying. The program runs for 30 years.
1952	President Truman establishes the National Security Agency (NSA), which absorbs the AFSA, to protect the nation. Part of its current mission: "to defeat terrorists and their organizations at home and abroad, consistent with U.S. laws and the protection of privacy and civil liberties
1967	*Katz v. United States*. The Supreme Court overturns the precedent set by *Olmstead v. United States*, determining that the Fourth Amendment does protect non-tangible possessions such as phone calls and electronic transmissions as well as the "reasonable expectation of privacy" in places like home, office, hotel room, phone booth. Examination of such places and things now require a warrant.
1968	Congress passes the Omnibus Crime Control and Safe Streets Act, the first federal law to restrict wiretapping. However, the law makes exception for the president's overriding authority to approve wiretaps if in the service of protecting the United States
1972	The Watergate Scandal begins on June 17, 1972, when five employees of President Richard Nixon's reelection campaign are caught breaking into the Democratic National Committee headquarters at the Watergate complex in Washington, DC. A Senate investigation and an inquiry by a special prosecutor follow.
1974	The House Judiciary Committee issues three articles of impeachment on July 30, indicting President Nixon for illegal wiretapping, misuse of the CIA, perjury, bribery, obstruction of justice, and other abuses of executive power. Nixon resigns before the proceedings conclude, thereby avoiding being removed from office.
1975	Headed by Senator Frank Church, the "Church Committee" investigates intelligence gathering by the CIA and FBI, uncovering hundreds of instances of warrantless wiretappings and unauthorized electronic surveillance.
1978	President Carter passes the Foreign Intelligence Surveillance Act (FISA), which establishes a secret court to hear requests for warrants for "electronic surveillance to obtain foreign intelligence information."
1986	An amendment to the Omnibus Crime Control and Safe Streets Act of 1968, the Electronic Communications Privacy Act (ECPA) adds wireless and data communications (cell phone conversations and internet communication) to the Act. Stored data more than 180 days old, however, is still vulnerable.

2002	The National Joint Terrorist Task Force (NJTTF) is created. A multi-agency collaboration, local task forces (JTTF) consist of "small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists" created to collect intelligence and combat terrorism.
2003	The passage of the Homeland Security Act by Congress in November creates the Department of Homeland Security, "a stand-alone, Cabinet-level department to further coordinate and unify national homeland security efforts." AT&T technician Mark Klein discovers a secret room at the company's facility in San Francisco. He later testifies in a federal lawsuit against the NSA by the Electronic Frontier Foundation that the room was set up to accomplish "vacuum-cleaner surveillance" of internet use of millions of unsuspecting Americans, without the consent of other carriers.
2005	*The New York Times* reveals government surveillance going back to 2002, including warrantless wiretapping of phone and internet of possibly thousands of Americans.
2007	2007 Protect America Act becomes law, amending FISA. The Department of Justice (DOJ) asserts that the legislation "restores FISA to its original focus of protecting the rights of persons in the United States, while not acting as an obstacle to gathering foreign intelligence on targets located in foreign countries. By enabling our intelligence community to close a critical intelligence gap that existed before the Act became law, the Protect America Act has already made our Nation safer." In October, President Bush issues the first National Strategy for Information Sharing (NSI).
2008	President Bush signs the FISA Amendments Act that allows immunity for telecom companies that cooperate with governmental information gathering and more.
2009	*The New York Times* reports that the NSA is involved in "significant and systemic" "overcollection" of domestic communications
2010	President Obama signs a one-year extension of expiring portions of the Patriot Act. In November, Secure Flight is established by the DHS to help streamline and make uniform the watch list system and is administered by the Transportation Security Administration (TSA). Prior to the implementation of Secure Flight, individual airlines were responsible for comparing passenger information with the government's watch lists (including the No Fly List (immediate threats) and the Selectee List (enhanced screening required)). WikiLeaks and other news organizations begin publishing excerpts from classified military documents captured by Private First Class Bradley Manning. Private Manning is arrested in May in Iraq and faces 21 counts related to the leaking of more than half a million documents, or "cables," related to the wars in Iraq and Afghanistan.

2011	A subpoena is issued for Twitter to furnish account information for individuals involved in the WikiLeaks disclosure of sensitive and confidential diplomatic cables. In May, Congress passes an extension of the Patriot Act. President Obama OKs the bill while in Europe.
2012	*The New York Times* reports an unprecedented public accounting of cell phone carriers: they responded to 1.3 million demands by law enforcement for subscriber information such as text messages and caller locations. The reports paint a picture of dramatic increase in cell phone surveillance over the last five years. Congress extends the FISA Amendments Act for another five years and also Obama signs off on the legislation.
2013	The *Guardian* reports FISA court judge Roger Vinson issues a secret order to Verizon to hand over "metadata"--time, duration, numbers called (without revealing the actual call content)—to the NSA for a three-month timeframe. *The Wall Street Journal* reports of similar arrangements with AT&T and Sprint. The *Guardian* and *The Washington Post* simultaneously reveal a secret program called PRISM, which was launched in 2009, that grants NSA access to the personal data of millions of people through Microsoft, Yahoo, Google, Facebook, Apple, and AOL. Two days later, on June 8, the Office of the Director of National Intelligence releases a three-page comment citing the FISA Amendments Act of 2008 as legal anchor. On June 21, the government files charges of espionage against Edward Snowden, a former NSA contractor, for the information leak. FBI director Robert Mueller admits that the United States employs drones as part of the domestic surveillance program. Speaking before a Senate Judiciary Committee, Mueller agrees that still-uncommon drone usage sparks concerns about personal privacy and is "worthy of debate and perhaps legislation down the road."
2014	On Jan. 17, 2014, President Obama announced reforms to the country's surveillance program based on the panel's recommendations. He said that while he believed the activities of the NSA were legal, he acknowledged that some compromised civil liberties. The reforms he outlined include: requiring NSA analysts to get a court order to access phone data unless in cases of emergencies; an eventual end to the collection of massive amounts of metadata by the government; the NSA will stop eavesdropping on leaders of allied nations; officials can pursue a phone number linked to a terrorist association by two degrees rather than three; and Congress will appoint advocates to argue on the side of civil liberties before the FISA court. He did not implement the recommendation about national security letters.
2015	A three-judge panel of the 2nd U.S. Circuit Court of Appeals in Manhattan ruled in May that Congress never authorized the bulk collection of the phone records of U.S. citizens when it passed the U.S.A. Patriot Act, and therefore the National Security Agency's program that does so is illegal. The panel allowed the program to continue, but called on Congress to amend the law. In the court's opinion, Judge Gerard Lynch wrote "knowledge of the program was intentionally kept to a minimum, both within Congress and among the public." The program was secret until 2013, when it was disclosed by Edward Snowden. The Senate votes, 67 to 32, to pass the USA Freedom Act, on June 2. The House had previously approved the bill, and President Obama signs it into law. The act ends the NSA's bulk collection of phone records of millions of Americans. That responsibility shifts to the phone companies, who can turn the data over to the government only when the Foreign Intelligence Surveillance Court issues a warrant to search the phone records of individuals

Appendix B

Dominant themes of pro-surveillance advocates in mainstream media

Authors	Professional Post	Political Leanings	Timing of Writings
Robert Gates	American Statesman; served as United States Secretary of Defense from 2006 to 2011; Lieutenant in the US Air Force; Deputy Director for NSA	Right	2014
Gerald Walpin	Inspector General of the Corporation for National and Community Service (beginning with Bush Admin. until his dismissal under Obama Administration	Right	2013
Daniel Byman	American author; Academic; Professional staff member for both the 9/11 Commission and the Joint 9/11 Inquiry Staff of the House and Senate Intelligence Committees; Former US government analyst	No affiliation detected	2014
James McAdams	Attorney; Academic	Right	2007

Appendix C

Dominant anti-surveillance advocates in mainstream media

Authors	Professional Post	Political Leanings	Timing of Writings
Glen Greenwald	American Author; Lawyer; Journalist	Left	2005-2014
Barton Gellman	American Author; Filmmaker and Journalist	Left	1999-2015
Heidi Boghosian	American Author; Lawyer; Former Blogger for Huffington Post; Humanitarian and Activist	Left	2013
John Cassidy	British-American Journalist	Left	2013