7-2020

Surveillance Technology Toward a Dystopian Future

Sandy Hernandez

SURVEILLANCE TECHNOLOGY TOWARD A DYSTOPIAN FUTURE

A Thesis Presented to
the Faculty of the University Honors Program
Northeastern Illinois University

In Partial Fulfillment of the Requirements
of the NEIU Honors Program
for Graduation with Honors

Sandy Hernandez
July 2020

HONORS SENIOR PROJECT
ACCEPTANCE AND APPROVAL FORM

Sandy Hernandez

Student Name

Surveillance Technology Toward a Dystopian Future

Title of Senior Project

This senior project has been reviewed by the faculty of the NEIU Honors Program and is found to be in good order in content, style, and mechanical accuracy. It is accepted in partial fulfillment of the requirements of the NEIU Honors Program and graduation with honors.

Faculty Advisor — 08/12/2020

Date

Faculty Reader — 08/12/2020

Date

Honors Curriculum & Standards Board — 08/12/2020

Date

Jon Hageman

Digitally signed by Jon Hageman
DN: cn=Jon Hageman, o=Northeastern Illinois University, ou=University Honors Program, email=jhageman@neiu.edu, c=US
Date: 2020.08.21 12:22:26 -05'00'

Coordinator, University Honors Program — 08/12/2020

Date

ABSTRACT

There is a continual debate between individuals who attempt to measure the individual's right to privacy against the government's right to know as an exchange to provide for the security of all citizens. Questions that demand an answer are whether the individual's right to privacy outweighs the government's duty to provide security; and if security is considered more important, can there even be a right to privacy. When questioning the right to privacy and state surveillance, there are three key goals. First, to investigate whether the human right to privacy should exist, considering the continued threat of terrorist attacks and public safety. Second, to question if state surveillance both actual and imagined are the fundamental means for governing state population, and individual citizens. Lastly, to assess if surveillance technology and state surveillance can be both a force of good and equal source of harm in society. To illustrate this debate, the focal point of this paper will be centered on power relationships in society as expressed through language (e.g., The Constitution) and practice (Laws). Therefore, this Honors Thesis Project surveys the historical background of surveillance technology and how the global surveillance industry uses its power to justify its decision-making in crisis's while violating Americans' civil liberties, human rights and inflicting harm.

TABLE OF CONTENTS

INTRODUCTION

For many, surveillance technology is a gateway for opportunities that lead to enhanced levels of public safety and national security (Introna, 2009). Surveillance technology capabilities have continued to grow exponentially. Presently, law enforcement and intelligence agencies use surveillance technology for criminal investigations to identify suspected criminals, locating wanted fugitives in a crowd, and or for spotting terrorists as they enter the country (Milovanovic, 2014). While some Americans support expansive surveillance within the government and law enforcement agencies and justify them as necessary for public safety and national security, other Americans feel that these actions pose violations to their civil liberties. In the context of surveillance technology, the inquiry is as follows: What was and is the situation surrounding surveillance technology? And how does the expansion in surveillance technology affect legality and constitutionality of Americans post 9/11 (Bamford, 2008)?

The right to privacy has been the subject of ongoing debate since the term was used by Samuel Warren and Louis Brandeis in 1890. The strength of the right to privacy reached its peak in the case *Griswold v. Connecticut* (381 U.S. 479), in which the Supreme Court explicitly stated that the right to privacy was covered by the Fourth Amendment. It can also be argued that the right to privacy can be defined with the First, Third, Fifth, and Ninth amendments. Although, there is a lack of complete agreement regarding the entitlement of privacy as right, particularly in a post 9/11 world (Bamford, 2008). There is a recurrent debate between the measure of an individual's right to privacy and the government's right to know information to provide security of all citizens. Constitutional privacy should not be seen simply as a procedural notion having no direct

relation to our more practical everyday uses of privacy. If, culturally, phone conversations are viewed as private, or decisions about contraception as being exempt from the judgement of other private citizens then it is logical to expect the Supreme Court to implement a "constitutional immunity from the judgment of the state within these narrowly restricted boundaries" (Humphry, 2018, p. 25).

The questions that beg to be answered are: If an individual's right to privacy offsets a government's obligation to provide security. Additionally, if national security is reasoned as a more significant or more pressing concern than the right to privacy, then can there be a right to privacy? Although, it is crucial to our nation's antiterrorism effort that our government (e.g., intelligence agencies) seize the legal opportunity to capture all forms of communication employed by terrorists and aggressive intelligence agents. Unavoidably, this will steer to less privacy for all citizens, and the examination that follows will mostly discuss the changes in the legal right to privacy that followed September 11, 2001.

It is crucial to analyze multiple aspects of society concerning domestic surveillance since it affects citizens' constitutional rights to privacy. The policies involved in the Patriot Act changed the privacy provisions found in the First and Fourth Amendments of the U.S. Constitution. The U.S. Patriot Act clashes with society, and privacy is the Patriot Act. The policies involved in the Patriot Act have changed the privacy provisions inherent in the First and Fourth Amendments. Therefore, a look to legal decisions that cite the Patriot Act in their justification or cite the Patriot Act's overstepping will show the state of the right to privacy *today* (U.S. Patriot Act, 2001).

This paper assumes a degree of familiarity with Foucault's main work but not its application to Information and Communication Technologies (ICTs) (Introna, 2009). Before we begin, it is essential to stress the provisionality of Foucault's ideas and the fact that Foucault himself was far from being a systematic thinker. He described his practices as "analytical work" rather than theory and his analysis of power relations as "not a theory, but rather a way of theorizing practice" (Foucault, 1977, p. 30). Many have reprimanded Foucault for what they see as lack of definition, yet at any rate some portion of the issue originates from his demeanor to language and discourse. Perhaps because he viewed language and discourse as unpredictable structures in which humanity can become *caught*; the experience of being caught inside a portion of Foucault's increasingly complex linguistic sentences parallel when compared. “Nothing is real, nothing has continuity- there's no such thing as liberty, "the concept of liberty is 'an invention of the ruling classes' and not fundamental to man's nature” (Foucault, 1977, p. 30).

This study situates the right to privacy and state surveillance as a form of what Michel Foucault called governmentality. Governmentality defines how a society is ruled, who rules, and under what conditions. When questioning the right to privacy and state surveillance, there are three key goals. First, to investigate whether the human right to privacy should exist, considering the continued threat of terrorist attacks and public safety. Second, to question if state surveillance both actual and imagined are the fundamental means for governing state population, and individual citizens. Lastly, to assess if surveillance technology and state surveillance can be both a force of good and equal source of harm in society. Through Foucauldian discourse analysis, conflicts in discourse frequently exist in systems with multiple interrelated and intersecting factors

affecting their trajectory and intensity. To illustrate this debate, the focal point will be centered on power relationships in society as expressed through language (e.g., The Constitution) and practice (Laws). The debate can be unraveled by focusing on the power relationships in society as expressed through language (e.g., The Constitution) and practice (Laws). Therefore, this the Honors Thesis Project surveys the historical background of surveillance technology and how the global surveillance industry uses its power to justify its decision-making in crisis's when violating Americans' civil liberties and human rights and inflicting harm.

LITERATURE REVIEW

History and Emergence of Surveillance Technology

Legislative acts and measures regarding U.S. surveillance can be dated as far back as the country's founding and was later transformed in the early 20th century. This historical period contributed significantly to communication advancements despite the onset of the two World Wars that occurred. Throughout these two World Wars, the use of radio technology for military operations expanded. The U.S. then developed the Cipher Bureau within the Military Intelligence Division, to assist with radio intelligence and cryptology—the study of codes and how to crack them. While disbanding the bureau happened in 1929, it was later reestablished as the core of the Signal Security Agency in World War II (Kamali, 2017). 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 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 US military intelligence agencies' transformation. 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, p. 50). In 1949, the Armed Forces Security Agency (AFSA) was created within the Department of Defense, responsible for organizing electronic communication throughout civilian agencies. In 1952, President Harry Truman initiated a memo that would transform the AFSA, due to ineffectiveness, at 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 United States' communications intelligence activities against foreign governments (Gallagher, 2013).

The Cold War-era marked another marked another transformative period for U.S. surveillance and intelligence-gathering agencies. Considering global communication advancements after World War II, along with Soviet fear and the potential use of nuclear weapons, the NSA's primary focus 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 pursue 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 (Myers & Staples, 2017).

It was not until 1968 that Congress passed the first federal law, the Omnibus Control and Safe Streets Act, to restrict wiretapping in 1968 (McNiff, 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 about government practice and Executive use of electronic eavesdropping. Pressures for reform within the political arena mounted, calling for more transparency (McNiff, 2013). Regarding national surveillance, however, the NSA remained relatively unknown to the American public.

It was in 1975, during 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 (McNiff 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* to identify foreign criminals (Myers & Staples, 2017).

In response to national concerns following the Watergate scandal, in 1978, Foreign Intelligence Surveillance Act (FISA) was signed into law to protect Americans (Cohn, 2013). Also, this Act was signed into law by President Carter (Gallagher, 2013). The Act established guidelines for the use of foreign intelligence surveillance. It authorized the creation of secret FISA courts to request warrants for electronic surveillance or domestic surveillance related to national security. Moreover, it determined that the only circumstances under which the U.S. and its intelligence agencies could lawfully conduct domestic surveillance would be for collecting foreign intelligence or foreign counterintelligence (Debenedetti, 2013).

In response to the commercialization of computers and technological advancements in wireless and data communications, an amendment to the Omnibus Crime Control and Safe Streets Act of 1968 was introduced. This Act was called the Electronic Communications Privacy Act (ECPA), later in 1986, the government was restricted from conducting wiretaps of cell phone and internet activity (Debenedetti, 2013). The Act also added new provisions about the access of stored electronic communications (McNiff, n.d.; Vicens et al., 2013). The most drastic transformation in U.S. surveillance came in the wake of the 9/11 terrorist attacks and the endorsement of the U.S. Patriot Act, which has had an immensely controversial and sustained global impact. The U.S. Patriot Act significantly expanded the U.S. government's authority to use surveillance domestically and internationally. This act removed many of the previous

restrictions in place for protecting personal privacy (Mcquade, 2016). Among other terms, 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).

The validity of this paper is contingent on four immediate changes that took place within the realm of legal surveillance under the Patriot Act are several. First, the government's ability to capture and retain personal records including libraries, bank statements, cell phone records, financial transactions, internet providers, etc (Toomey, 2018). Second, the expansion of the government's ability to search private property before notification of the owner. Third, the ability for all government agencies (i.e., FBI), to conduct physical searches and wiretaps on American citizens with the intent to attain evidence of a crime without probable cause. Fourth, the expansion of the Fourth Amendment exception for spying that reduces judicial oversight and interprets *addressing* information in a manner that authorizes the tracking and accumulation of personal URL and internet activity (U.S Patriot Act, 2001).

Today, the Act continues to impact the relationship between Americans and surveillance technology. In May 2020, the U.S Patriot Act was reauthorized by Congress, meaning that it will continue to grant sweeping surveillance powers that will allow national-security agencies to spy on the communications of millions of people in the United States (Nadler, 2020).

The debate over state surveillance in the post 9/11 era has generated a historical inquiry on the formation and growth of federal law enforcement and intelligence agencies such as the FBI, CIA, and NSA and their surveillance practices and patterns on

Americans. Thus, the data mentioned is divided in three parts: 1.) data patterns of surveillance, 2.) the function of corporate service providers, and 3.) shaping public perceptions (Boghosian, 2013).

Data Patterns of Surveillance

The trend toward increasing government surveillance became evident with news about the Secret Court of FISA, which authorizes citizens' undisclosed surveillance. 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 personal financial records, medical records, and even library records. (Greene, 2011, p. 40)

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

> 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 the 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. (Austin, 2014, p. 22)

In the post 9/11 era, government surveillance has also tended to intrude in financial surveillance. Data indicate that under national security considerations, government surveillance of financial records has vastly increased. Released data from the Treasury Department that 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. Scholars suggest that financial surveillance is an overreach beyond monitoring terrorism. Much of the legislation currently being enforced concerning surveillance, is a retraction from the earlier measures intended to protect citizen privacy in a digital era (Finley & Esposito, 2014).

The Privacy Act provided safeguards for citizen privacy with government and financial institutions (U.S 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. Besides, the 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 about financial transactions. By 1993, the Clinton administration ushered into the system new and more robust encryption standards developed by the NSA (Freeman, 1995). The introduction of the Clipper Chip was central to the new standard. The Clipper

Chip was a cryptographic device specifically aimed to protect private communications. However, simultaneously permitting government agents to obtain the "keys" upon presentation as "legal authorization" (Electronic Privacy Information Center, 2020, p. 4). Meaning, that these ‘keys’ enabled the government to access encrypted communication and voice transmissions. Similarly, capstone was another type of chip developed for data using algorithms. The installation of the clipper chips was the semiconductor in all computer modems, fax machines, and telephones that facilitated the encryption of communications data (Freeman, 1995).

As early as 1977, particularly regarding financial transactions, The National Bureau of Standards required encryption procedures to protect computer data (Freeman, 1995). 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 can quickly unlock this information if desired. Moreover, as security measures heighten, the concentrated power that these master keys represent is placed in the hands of fewer and fewer people.

Function of Corporate Service Providers: Corporatocracy

The second part of the data relevant to the present inquiry deals with a private corporation's role, specifically by service providers from the information technology industry in the growth of surveillance post 9/11. (Toomey, 2018) The principal security technologist in the Privacy and Technology Project of the American Civil Liberties Union (ACLU), Soghoian, noted a close relationship between government surveillance and the private information technology industry sector (Saghoian & Bort, 2009). Internet

firms and telecommunications carriers receive monetary compensation from the government when disclosing customer information to law enforcement officers (Saghoian & Bort, 2009). Saghoian and Bort (2009) stated:

> Cox Communications, the third-largest cable provider in the United States, is the only company I have found that has made its surveillance price list public. Thus, we can 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 are 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 of years ago. (p. 60)

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. (Santos & Lopes, 2019). Data suggests that the involvement of the private sector information technology industry in government surveillance has been on the rise (Toomey, 2018). Also, published information on PRISM, an electronic mass surveillance program initiated by the US government in 2007; PRISM works in conjunction with telecommunications companies to monitor and store various forms of electronic communications both domestically and abroad. The ways that government gathers this information above, does not require individual warrants since it has broad approval by the secret FISA court (Toomey, 2018).

One area that raises issues is the collection and analysis of personal information under the Foreign Intelligence Surveillance Act (FISA). Little, however, is known due to the secrecy clause and secretive nature of the FISA courts (House, 2019). The information that is known is only what law enforcement agencies are willing to disclose Because of the secrecy clause, unless government agencies choose to disclose such information, it is likely that the public will never know the extent to which law enforcement agencies request records containing personal information from various organizations. As a result, the public will not know the extent to which agencies are engaging in information collection, analysis, and sharing activities within and across agencies as well as across levels of government and sectors (Boghosian, 2013). To what extent do individuals have the right to know when their private information (their privacy) has been accessed? This is an important dimension to the debate, and how it is answered will determine to what extent is there is a right to privacy, particularly relating to the technology industry.

In the Age of Surveillance Capitalism, Dr. Zuboff (2020), integrates the themes of capitalism and the digital revolution. Dr. Zuboff (2020) discusses the traumatized history of U.S. tech companies that damaged the industry. Explaining how Apple's success and its electronics sold on the concept of consumer choice. Apple thrived financially primarily due to the surveillance conditions created by the U.S. National Security Agency (NSA) and the CIA's financial interest in investments directed at initiatives to fight war on terror. All these elements, Zuboff claims, this thrust capitalist investment and market expansion of the tech and surveillance market industry. The companies, created by Mark

Zuckerberg and Larry Page, are known as tech-giants that developed surveillance capitalism.

Zuboff (2020), coined term, surveillance capitalism, pertains to economic and social logic. The definition of surveillance capitalism is "individually claims human experience as free raw material for translation into behavioral data [which] …are proprietary behavioral surplus, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into prediction products that anticipate what you will do now, soon, and later" (p. 200). Surveillance capitalism connects to the debate of expanded power from the government due to the Patriot Act because both were used to establish conditions under which the government could electronically monitor various types of ongoing communications within the United States in non-emergency situations (e.g., technology companies who collect data) (Freeman, 1995).

Zuboff (2020) begins by explaining and contrasting the concept of 'instrumentarian power' to totalitarian power. She explained that instrumentarian power is a consequence of surveillance capitalist operations that serve to put at-risk one's autonomy and democracy. Zuboff argues that neither privacy nor antitrust laws provide adequate protection from the unprecedented practices of surveillance capitalism. The threat to privacy is not implicit in the legislation but only a possibility if safeguards are not put in place (Conniry, 2016). The Fourth Amendment is probably going to be satisfied on the surface, but too much has been left to the discretion of the executive branch. This can be measured by looking like the actual legislation under both FISA and the Patriot Act and how the Fourth Amendment is now applied (post 9/11); subsequent chapters will look further into this issue. The checks and balances system of American

government was created to keep each branch (executive, legislative, and judicial) in equal parity with no branch too weak or too powerful (Freeman, 1995).

The executive branch may try to increase its power especially through post 9/11 legislation, but within the balance of government it cannot be described with having too little power. American history teaches how dangerous it is to allow the executive power to conduct electronic surveillance unchecked. Thus, where executive power has increased, Americans should be concerned that privacy may be unnecessarily threatened as a result (Debenetti, 2013).

Unlike industrial capitalism, which profits from exploiting natural resources and labor, surveillance capitalism profits from the capture, rendering, and analysis of behavioral data through 'instrumentarian' methods designed to cultivate 'radical indifference […] a form of observation without witness' This allowed surveillance capitalists to access a vastly untapped source of information when data collecting for internal analytics and programming. They took this new resource and turned it into a lucrative financial opportunity: they could sell that 'data exhaust' to advertisers (Zuboff, 2020).

In a capitalist society and the tech industry, information, such as a user's likes and dislikes, gathered through social platforms like Facebook, are freely used by that platform to shape user experience through an algorithm (Zuboff, 2020). However, the danger of surveillance capitalism is that platforms and tech companies having entitlement to this information because it is free for them to access. There is a lack of accountability, and minimal supervision by governments and users themselves. And so, the relationship between data and surveillance raises a moral implication. For instance, Google

introduced a feature that used "commercial models…discovered by people in a time and place" (Zuboff, 2020, p. 15). Digital marketing is targeting people through a smartphone but also work hand in hand with one's environment and habits, for instance, such as getting an advertisement of a local bar when walking around downtown in the evening. Advertising attempts this technical and specific can quickly impact one's decision-making process in the activities they choose and in political decisions. Furthermore, the freedom granted to tech companies comes from the idea that "surveillance capitalism does not abandon established capitalist 'laws' such as competitive production, profit maximization, productivity and growth" are principles any business in a capitalistic society should aim to excel in, to be competitive (Zuboff, 2020, p. 119).

Shaping Public Perceptions

When discussing the role of corporations and the relationship between the government and surveillance technology, one must examine digital companies. The rationale is to observe the precarious relationship between privacy and decision making (Scott, 2012). The following examples structure the patterns in public perceptions concerning privacy, surveillance technology, and decision making.

In *Nudge: Improving Decisions About Health, Wealth, and Happiness,* Thaler and Sunstein (2009) begin by discussing a framework of Libertarian Paternalism. A concept that is accepting of governments or authorities shaping and influencing of citizen behavior and decision making. To 'nudge' people into making better decisions through any technological means, altering the default and decision criteria made available to them. For instance, the authors state, "perhaps setting your 401k account to default to the maximum savings rate would be better for you than allowing the default withdrawal to be

$0" (Thaler & Sustein, 2009). This example demonstrates the concept of digital marketing as the 'nudge.' In other words, the 'nudge,' when analyzed across multiple industries and situations, points out reoccurring influence of digital decision making. Presently, it happens with almost every product or tech gadget purchased (Thaler & Sustein, 2009).

In sum, the data demonstrate an increase in quantity 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 have a financial interest in technological innovation to secure their competitive advantage. It is important to note a possible future outcome with concentrated power and the increase of surveillance technology.

Consider the following example to show a dystopian future that depicts the lack of privacy. In *Homo Deus,* Harari (2015) outlines the future. From Harari's point of view, future society will, be influenced and ultimately governed by human cyborgs, Ai, algorithms, and cyber bots enhanced to be superior to Homo Sapiens. To illustrate, Harari (2015) poses the following question: "As we live longer and embrace the opportunities of life-expanding and ability-expanding genetic encoding, what can we expect" (p. 25)? Harari states that as more information, data, and knowledge is disseminated and becomes increasingly available, the rise of super-human capabilities and cyborgs will become an essential human issue. Harari states, "In the past, genius-level intellects had access to only so much data, but soon, they may have all the data and all the brain-power, which would (optimistically) be amazing or (not as optimistically)" (p. 45). It could preempt the end of humanity, and as the world, we know it.

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.

Meta-analysis 1. 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 U.S. is operating its own interpretation of the law, as it is enshrined to, citing the imperative of national security" (p. 53).

Meta-analysis 2. Pro-surveillance advocates have further claimed that hi-tech surveillance and intelligence gathering is a very powerful tool that has enabled the U.S. government to identify, and effectively prevent terrorists from attacking America, and, as such, support that electronic surveillance should continue and expanded if able. Therefore, pro-surveillance advocates appear to see anti-surveillance advocates as ideological 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.

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 U.S. government has reached such extreme levels that it threatens democracy in general, and the democratic rights of American citizens (Boghosian, 2013). 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.

Meta-analysis 1. Opposition to the pro-surveillance advocates, and many anti-surveillance advocates view government surveillance, particularly considering current revelations, as an overreach, abuse, and violation of governmental power that threatens democracy and the rights of American citizens (Boghosian, 2013). Many premises 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" (p. 55). 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). Like 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, 2013).

Meta-analysis 2. In addition, anti-surveillance advocates contend that the extent to which the U.S. government has been engaging in surveillance, both domestically and internationally, is unconstitutional and a violation of human rights, particularly regarding citizens' rights to privacy (Bamford, 2008; Boghosian 2013). They argue that unimpeded mass surveillance is 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, 2013). 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, 2013).

Court Cases and the National Security Agency (NSA)

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 Freedom Work'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). Senator Rand Paul, who has also been a strong opponent of the U.S. Patriot Act since its commencement, criticized the government's ability to search, the phone records of Americans. Senator Rand 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, he claims there is unequal and subjective nature to this debate because, it has yet to take place primarily between government officials and representatives of the NSA, without citizen participation (McCalmont, 2014).

State Surveillance and Privacy

Opinion and literature within the social sciences has often promoted technology, and the information revolution 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 (Castell et al., 2015). A prerequisite for addressing this issue is a basic understanding of the mode of technological advancement and diffusion into society.

Michel Foucault, a philosopher, was influenced by Bentham's panoptic schema. The key concept of Bentham's work, a person conceiving he is being watched even when he may not be. Foucault expands this key concept because he considers power and the application thereof when he says, "He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection" (Foucault, 1977, p. 66). His concept is the subject of surveillance, because he knows he is being watched, will take care to police himself. Ultimately the subject will internalize the notions of power, monitor himself and conform from within the body. In short, the panoptic schema is about the assertion of power over and in individuals. (Foucault, 1977).

Part of the surveillance infrastructure is built into privacy policy. Perceptions and definitions of privacy have evolved over time, but a recent study found a group of key terms that Americans consider when they think of privacy. "Among all of the themes referenced in the open-ended responses to the online survey, security, safety and protection was the most frequently-referenced category" (Pew Research Center, 2020, p. 14). As more activities go online, industries and businesses today are increasingly adapting their privacy policies. The privacy policy is a statement of what is collected, how it is collected and what is done with that information when you use that online service or interact with that website. One study found that publication of a privacy policy inherently meant that a user's privacy was protected. "62% of respondents to a survey believed (incorrectly) that the existence of a privacy policy implied that a site could not

share their personal information without permission, which suggests that simply posting a policy that consumers do not read may lead to misplaced feelings of being protected" (Walters, 2016, p. 25).

At the same time, "Beyond social networking sites, Americans express a broader loss of control over the way their personal data is managed by companies. Fully 91% of adults "agree" or "strongly agree" that "consumers have lost control over how personal information is collected and used by companies" (Pew Research Center, 2020, p. 14). These two studies show the data self is confused and frustrated with the manipulation of privacy online. Further, a default setting is often highlighted at the time a choice of agreement is being made. The default setting is suggesting a normative behavior. Sticking to default settings is convenient, and people often interpret default settings as implicit recommendations. Thus, it is not surprising that default settings for "one's profile's visibility on social networks, or the existence of opt-in or opt-out privacy policies on websites, affect individuals' privacy behavior" (Brandimarte & Acquisti, 2012, p. 30). In some instances, users are presented with the opportunity to decide, to 'agree' to the policy and be permitted to use the service or 'disagree' and be directed away from the site (e.g., Facebook). Depending on the importance of the site to the user, this decision is not a decision as much as a resignation of privacy.

CONCLUSION

Finally, it may be concluded that the discussion on surveillance remains intricately complex and open for debate. The historical background of the adoption and expansion of U.S. surveillance technology in a pre-9/11 and post 9/11 context in the literature examined reveal critical themes about the government's involvement with surveillance technology are an invasion of privacy, limited supervision, and capitalistic business models in the global surveillance industry. Also, the research reveals the needed attention to the violation of Civil Liberties and Human Rights. A sense of urgency connected with the expansion of technology, limited supervision, and the lack of public awareness of how American citizens are implicated in the future.

The surveillance technology and state surveillance vs. Security and Privacy paradox does not have to be. In reality the debate over the tradeoff between the right to privacy and national security ended many years ago. Privacy has been lost for some time now. We have been voluntarily giving away our data, and our private lives at will and are only now becoming aware of this reality. The right to privacy and protection against unlawful search and seizure, once assumed as a given right and protected under the Fourth Amendment of the U.S. Constitution, has nearly disappeared as electronic or technology surveillance of the public has expanded to include everyone in the country regardless of suspicion or court-ordered warrant. Personal privacy, once easy to sustain, has become increasingly difficult to keep living in the digital age. Americans are being left in the dark surrounding domestic surveillance (Gellman, 2020). There personal information of all Americans is covertly collected, categorized, commoditized, bought, and sold.

As Foucault suggests, goals of efficiency, automation, and continuous function are in play now more than ever. Technology, surveillance, and computing systems are becoming faster and more powerful (Caluya, 2010). The continued growth of analytics software has shown improvements in efficiency and automation (Losavio et al., 2015). As a result, the development, use, and expansion of these smart devices enable continuous observation, diminish privacy, and fuel the perpetuation of the continuous observation to support the global surveillance industry. Critics have criticized Foucault for what they see as his permanent obscurity, part of the problem comes from his attitude to language and discourse. Discourses are complex structures in which people can become *trapped*; perhaps the experience of being trapped inside Foucault's more difficult sentences is meant to echo this.

Today, surveillance technology compromises the privacy and constitutional rights of all Americans. As a country, the founding fathers held that any elite should experience constraints upon its power, and there is no power-equalizer higher than knowledge. Many Americans have yet to realize the coercion and manipulation of state surveillance and the way they use surveillance technology byways of the U.S. patriot act. Imagine if we inversed surveillance for citizens to have the capacity to keep surveillance over governments and state actors. Aa a way to be able to watch the watchers. By doing so, would it give way to a power balance by creating an equal, transparent society and keep them in check? A state where personal freedoms and justice are equally distributed, maximizing privacy, national security. Until then, surveillance technology will continue to compromise the privacy and security rights of all Americans. Surveillance technology

compromises the privacy of citizens. Furthermore, Americans do not realize the manipulation because of fear and no understanding of the Patriot Act's effects.

REFERENCES

Anttiroiko, A.-V. (2019). Castells' network concept and its connections to social, economic and political network analyses. *Journal of Social Structure*, *16*(1), 1–18. https://doi.org/10.21307/joss-2019-021

Austin, L. M. (2014). Lawful Illegality: What Snowden Has Taught Us About the Legal Infrastructure of the Surveillance State. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2524653

Bamford, J. (2008). *The shadow factory: the ultra-secret NSA from 9/11 to the eavesdropping on America*. Find in a library with World Cat. https://www.worldcat.org/title/shadow-factory-the-ultra-secret-nsa-from-911-to-the-eavesdropping-on-america/oclc/229309155.

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

Bostock, B. (2019, June 11). *'1984,' George Orwell's classic dystopian nightmare was published 70 years ago. Here are 5 eerie predictions that came true.* Insider. https://www.insider.com/george-orwell-1984-what-came-true-2019-5.

Bandmate, L., & Acquits, A. (2012). The Economics of Privacy. *Oxford Handbooks Online*. https://doi.org/10.1093/oxfordhb/9780195397840.013.0020

Calusa, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies. *Social Identities*, *16*(5), 621–633. https://doi.org/10.1080/13504630.2010.509565

Castell, Freeman, & Scott. (2015, July). *(PDF) Castells' network concept and its connections to ...* Journal of Social Structure.

https://www.researchgate.net/publication/298709800_Castells'_network_concept_and_its_connections_to_social_economic_and_political_network_analyses.

Castells, M. (2010). http://www.citethisforme.com/topic-ideas/sociology/Network Society and Social Movements-19308487.

Conniry, K. L. (2016). National Security, Mass Surveillance, and Citizen Rights under Conditions of Protracted Warfare. National Security, Mass Surveillance, and Citizen Rights under Conditions of Protracted Warfare.

Corrigan, J. (2019, June 20). *DHS to Move Biometric Data on Hundreds of Millions of People to Amazon Cloud*. Nextgov.com. https://www.nextgov.com/it-modernization/2019/06/dhs-move-biometric-data-hundreds-millions-people-amazon-cloud/157837/.

Debenetti, G. (2013, June 7). *Factbox: History of mass surveillance in the United States*. Reuters. https://www.reuters.com/article/us-usa-security-records-factbox-idUSBRE95617O20130607.

Deeks, A. S. (2017). Regulating Foreign Surveillance through International Law. *Oxford Scholarship Online*. https://doi.org/10.1093/oso/9780190685515.003.0018

Encyclopædia Britannica, inc. *Church Committee*. Encyclopædia Britannica. https://www.britannica.com/topic/Church-Committee.

Finley, L., & Esposito, L. (2014). "Digital Blackwater": The National Security Administration, Telecommunications Companies and State-Corporate Crime. *State Crime Journal*, *3*(2), 182. https://doi.org/10.13169/statecrime.3.2.0182

Fitzgerald, K., Stone, O., & Talbot, D. (2016). In *Snowden: the only safe place is on the run: Joseph Gordon-Levitt/Shailene Woodley*. New York, NY; Skyhorse Publishing.

Freeman, E. H. (1995). When Technology and Privacy Collide. *Information Systems Security*, *4*(3), 62–66. https://doi.org/10.1080/10658989509342511

Gao, G. (2020, May 30). *14 striking findings from 2014*. Pew Research Center. https://www.pewresearch.org/fact-tank/2014/12/22/14-striking-findings-from-2014/.

Gellman, B. (2020, May 19). *Dark Mirror: Edward Snowden and the American Surveillance State: Hardcover*. Barnes & Noble. https://www.barnesandnoble.com/w/dark-mirror-barton-gellman/1122928803.

Gray, D. C. (2017). THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE. In *the Fourth Amendment in an Age of Surveillance* (pp. 314–314). afterword, DigitalCommons@UM Carey Law.

Greene, R. (2012, February 17). *When Is Enough Enough? Government Surveillance Skyrockets in 2010.* American Civil Liberties Union. https://www.aclu.org/blog/national-security/privacy-and-surveillance/when-enough-enough-government-surveillance.

Harari Yuval Noaḥ. (2018). “Sapiens: A Brief History of Humankind,”. In *Homo deus: a brief history of tomorrow* (pp. 239–245). essay, Harper Perennial.

Humphry, J. (2018, November 9). *(PDF) Exclusion by design: intersections of social, digital and data exclusion*. ResearchGate.

https://www.researchgate.net/publication/333054051_Exclusion_by_design_intersections_of_social_digital_and_data_exclusion.

Introna, L. D. (2009). Making sense of ICT, new media, and ethics. *Oxford Handbooks Online*. https://doi.org/10.1093/oxfordhb/9780199548798.003.0013

Kamali, S. (2017). Informants, Provocateurs, and Entrapment: Examining the Histories of the FBI's PATCON and the NYPD's Muslim Surveillance Program. *Surveillance & Society*, *15*(1), 68–78. https://doi.org/10.24908/ss.v15i1.5254

Kim. (2019). Younger Generations are Infected by Continuous Socialization to Accept Diminished Privacy: A Global Analysis of How the United States' Constitutional Doctrine Is a Main Contributor to Eroded Privacy. *Indiana Journal of Global Legal Studies*, *26*(1), 335–339. https://doi.org/10.2979/indjglolegstu.26.1.0335

Lieven, A. (1970, January 1). *America right or wrong: an anatomy of American nationalism: Lieven, Anatol: Free Download, Borrow, and Streaming*. Internet Archive. https://archive.org/details/americarightorwr00liev.

Losavio, M., Song, Y. /, James, J. I., & Chow, K. P. (2015, April 1). *(PDF) A World Information Order - Privacy and Security in a Hyper-Networked World of Data and Analysis*. ResearchGate. https://www.researchgate.net/publication/283563769_A_World_Information_Order_-_Privacy_and_Security_in_a_Hyper-Networked_World_of_Data_and_Analysis.

Margulies, P. (2017). Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy. *Indiana Journal of Global Legal Studies*, *24*(2), 459. https://doi.org/10.2979/indjglolegstu.24.2.0459

Mcquade, B. I. (2016). Police and the Post-9/11 Surveillance Surge: “Technological Dramas” in “the Bureaucratic Field.” *Surveillance & Society*, *14*(1), 1–19. https://doi.org/10.24908/ss.v14i1.5291

Milovanovic, D. (2014). *Quantum Holographic Criminology: Change in basic assumptions in criminology, law, and transformative justice*. Carolina Academic.

Myers, A. J., & Staples, W. G. (2017). Review of Reeves' Citizen Spies: The Long Rise of America’s Surveillance Society. *Surveillance & Society*, *15*(5), 693–694. https://doi.org/10.24908/ss.v15i5.7009

Peacock, V. (2010). Karen Barad, Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning. *Opticon1826*, (8). https://doi.org/10.5334/opt.081013

Rao, U., & Nair, V. (2019). Aadhaar: Governing with Biometrics. *South Asia: Journal of South Asian Studies*, *42*(3), 469–481. https://doi.org/10.1080/00856401.2019.1595343

Rubin, G. (2011). *Freedom and order: how democratic governments restrict civil liberties after terrorist attacks--and why sometimes they do not*. Find in a library with WorldCat. https://www.worldcat.org/title/freedom-and-order-how-democratic-governments-restrict-civil-liberties-after-terrorist-attacks-and-why-sometimes-they-dont/oclc/721962345.

Santos, R. P. D., & Lopes, G. R. (2019). Thematic series on Social Network Analysis and Mining. *Journal of Internet Services and Applications*, *10*(1). https://doi.org/10.1186/s13174-019-0113-z

Scott, L. (2012). Reflections on the Age of Intelligence. *Intelligence and National Security*, *27*(5), 617–624. https://doi.org/10.1080/02684527.2012.708512

Simon, M. (2016, April 25). *H2O*. An Overview of The Griswold v. Connecticut (1965) Case: By Madeleine Simon. https://h2o.law.harvard.edu/text_blocks/27514.

Thaler, & Sustein. (2009). Introduction. In *Nudge: improving decisions about health, wealth, and happiness: Rev. and exp. ed* (pp. 6–11). essay, Penguin.

Thompson, M. (2004, March). *Discourse, 'Development' & the 'Digital Divide': ICT & the ...* Jstor. https://www.researchgate.net/profile/Mark_Thompson25/publication/263380774_Discourse_'Development'_the_'Digital_Divide'_ICT_the_World_Bank/links/5561a8f408ae86c06b64c452.pdf.

Toomey, P. (2018, August 23). *The NSA Continues to Violate Americans' Internet Privacy Rights*. American Civil Liberties Union. https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy.

Zuboff, S. (2020). Chapter 6. In *The age of surveillance capitalism: the fight for a human future at the new frontier of power* (pp. 117–121). essay, PublicAffairs.