Information Technology: National Security Savior or Civil Rights Disaster

By

Celeste Brevard

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Arts Program in International Relations New York University December 2020

Dedication:

For my husband who has always encouraged me to ask the difficult questions and has helped me find the answers. His degree in computer science was vital to understanding the innerworkings of the technologies dissected in this paper. Also, to my sister, my steadfast editor and supporter.

Finally, to my professors Colette Mazzucelli and Asli Peker for guiding this research.

Abstract:

The balance between state security and individual liberty is a line the United States has had to walk carefully. Protecting the populace while staying true to the values laid out in the Constitution and the Declaration of Independence have become increasing challenging after September 11th. However, the combination of disaster diplomacy tightening the reigns on privacy after terrorist attacks and the onset of a global pandemic are further encouraging the development of surveillance technology and a pervasive "internet of things." These are changing the dynamic between technology and privacy. Corporations have begun collecting personal data to use as a form of "surveillance capitalism." This is making it increasingly difficult for citizens around the word and even in the "city on a hill" to hold on to the privacy component of their civil liberties. Compared to the authoritarian rule in China, in which privacy of the individual has been secondary to that of the collective good since the instalment of the Chinese Communist Party, stark contrasts in data collection and privacy rules should be clear. However, corporations in the United States are working with the government either inadvertently or directly making their all-encompassing collection of data for corporate profit too similar to that of the Chinese government. This thesis analyzes the use of information technology by China and the United States to gauge whether the type of political regime these new technologies are being created under makes a difference in terms of the civil rights of its populace. This is done by examining practices of states and corporations in each country and evaluating the impact they have had on the populace as well as the effectiveness of the technology.

Table of Contents

Introduction: Surveillance Technology: Tool for State Security or a Civil Rights Concern?

According to Freedom House, global internet freedom is in its ninth year of decline as of 2019. The United States is in its third year of decline and it was determined China had the worst internet freedom abuses in the world. This declaration is a direct contradiction of the space that Sir Tim Berners-Lee--the inventor of the World Wide Web--thought he had created. Along with other early web developers and users, Sir Berners-Lee's goal of decentralization that would bring "freedom from indiscriminate censorship and surveillance"[1] has been replaced with a trend "toward illiberalism, exposing citizens to an unprecedented crackdown on their fundamental freedoms."[2] When the internet was created, it was exported with the fundamental ideals of a democracy. It would be a space where people could collaborate, inform, and connect. However, as Julie E. Cohen has made clear in her book *Between Truth and Power: The Legal Constructions of Informational Capitalism* neoliberal forces have morphed this changing technology and the laws meant to regulate it to align "with the efficiencies that powerful interests have identified and the rationalizations they advance to frame particular kinds of change as desirable."[3] Could this shift be the result of the ideas laid out in "A Declaration of the Independence of Cyberspace" in which John Perry Barlow, a cyberlibertarian and philosopher states, "Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here?"[4] Was it the September 11th attacks and the "age of terror" that created this dichotomy as sociology professor and Director of the Surveillance Studies Center David Lyon states in *Surveillance after September 11?* Or is the change in global competition and the shift from conventional warfare to cyberspace

[1] World Wide Web Foundation, "History of the World Wide Web."
[2] Freedom House, "Freedom on the Net 2019: The Crisis of Social Media."
[3] Cohen, *Between Truth and Power,* 4.
[4] Ibid. 238.

with the internet posing a threat to “the right of a state to govern itself without external interference,”[5] as James Andrew Lewis Director of the Technology and Public Policy Program at the Center for Strategic and International Studies suggests? Regardless of the cause, this trend’s supporters are in favor of increased state security due to the role international terrorism still plays in the world. Critics warn of global civil rights implications if these shifts are not closely monitored. Each of these arguments are constructed within the parameters of the regime in which the technology is being utilized. This thesis examines the relationship between state sponsored surveillance and corporate surveillance and its impact on democracy by conducting a comparative analysis of this relationship in China and the United States. These countries were chosen as they develop, implement, and export information technology.

Proponents of state-centered information technology argue that the security of the state and the individuals within are being protected by these measures. Li Shulei, Deputy Secretary of the CPC Central Commission for Discipline Inspection and Vice Head of the NSC, called for legal assistance through international law to support programs like “Sky Net 2019.” This program was created, according to her declaration to “capture more fugitive suspects and prevent more corrupt officials from fleeing.”[6] Sky Net, which placed millions of cameras in cities all over China to create a police system powered by big-data, has made some Chinese citizens feel more safe.[7] According to the Center for Strategic and International Studies, Huawei’s “Safe Cities” experienced a 15% decrease in violent crime, 41% increase in cases being solved and an increased emergency response time down from 10 minutes to 4.5. This led to “citizen

[5] Lewis, “Cognitive Effect and State Conflict in Cyberspace,” 1.
[6] Xinhua, “China Launches "Sky Net 2019" to Capture Fugitive Officials.”
[7] Mozur, “Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras.” This concept will be further explored on page 30.

satisfaction" increasing from 60.2% to 98.3% according to Huawei's reports.[8] These systems were created in parallel to the increased ethnic tensions in China. Similarly, after September 11th, the government and law enforcement agencies in the United States began utilizing private businesses' information technology in their fight against Al Qaeda. John Yoo, a former government official and lawyer, wrote an article entitled, "The Legality of the National Security Agency's Bulk Data Surveillance Programs" for the Harvard Journal of Law and Public Policy in response to Snowden's 2013 leak of the NSA programs justified by the Patriot Act. He argues that the attacks that occurred on September 11th changed the way in which the President must search for potential threats to the state. In the piece he calls for the government to simply be allotted the same access to information as users of any website. That entails detailed access to information about those using the site. He begs the question, "Is the government's effort to find violent terrorists a less legitimate use of such data?"[9] Yoo also states that the issue with the Patriot Act and the Foreign Intelligence Surveillance Act before the 2008 amendments is that they did not go far enough. He points out that non-state actor "armies" do not fall under the "probable cause" requirement nor do they allow for the detection of Al Qaeda members as some actors may not have the criminal record necessary to monitor them. Thus, he calls for more sweeping use of current data collection technology.[10] While Yoo has become a controversial character in some circles, he was not alone in his assessment. The Senate in a hearing on technology and terrorism in 2002 thanked the members for giving them the tools such as, "the provision allowing Internet providers to disclose records to law enforcement in emergencies preventing risk of life."[11] Despite the clear implications of terrorism on the collection of user

[8] Hillman, and McCalpin, "Watching Huawei's 'Safe Cities.'" "Safe Cities" will be analyzed in Chapter 3.
[9] Yoo, "The Legality of the National Security Agency's Bulk Data Surveillance Programs," 929.
[10] Ibid.
[11] Senate No., "Subcommittee on Technology, Terrorism, And Government Information of The Committee," 9.

information without their knowledge or consent, “Contemporary legal and policy discussions about the internet and digital technologies, however, nonetheless have retained more than a little of their original idealism.”[12]

Those opposed to this use of technology stress the consequences on civil rights and democracy as reasons why this technology should be monitored and regulated. This opinion comes from those in a range of fields and organizations. These include human rights organizations, journalists, and scholars. While these concerns will be addressed in the body of the thesis, most of the research uses the concept presented by Shoshanna Zuboff as the basis for analysis. Zuboff, a Harvard professor, presents the idea of “surveillance capitalism” as a consequence of the shift from industrialism to informationalism. This notion was first presented by sociologist Manuel Castells and reiterated by Julie E. Cohen in *Between Truth and Power* as “information capitalism.” Surveillance capitalism is the collection of human experience presented through data. This is provided by users when consenting to blanketed user agreements, or without their knowledge or consent altogether. Surveillance capitalism and information capitalism are similar notions. Zuboff, however, focuses less on the market impacts which are emphasized in information capitalism and instead highlights the behavioral implications. She describes this process by stating, “behavioral surplus, fed into advanced manufacturing processes known as “machine intelligence,” fabricated into prediction products that anticipate what you will do now, soon, and later…In this way, surveillance capitalism births a new species of power that I call... Instrumentarian power [this] knows and shapes human behavior toward others’ ends.”[13] When taken together, Zubofff and Cohen’s analysis imply that private business is not

[12] Cohen, *Between Truth and Power*. 4.
[13] Zuboff, *Surveillance Capitalism*. 15.
Instrumentarian power is the harnessing of the behavioral information gathered through surveillance capitalism.

only exerting power over individual action but also influencing institutional law and political power in their favor. Thus, the consequence is both the influence of individual political and market decisions as well as the inability to properly regulate the use of data because of the wide-ranging influence of these businesses in governance through political and capitalistic power. The United States Congress has begun to understand the implications of this technology on individual liberties, but only when framed in an international context.

In a hearing on political and human rights in China, Congress proclaimed, "The Communist Party has built an Orwellian surveillance State in Xinjiang that is gradually being adopted perhaps over—across China, and even worse may be a Chinese export."[14] While framed as a hypothetical, the exportation of Chinese surveillance technology is a fact. As is the implementation of similar technology in the United States. These impacts are compounded by the cooperation of American businesses with China's authoritarian regulations. China's Belt and Road initiative focuses on increasing their technological prowess globally. To gain access to Chinese markets, "companies must conduct increased surveillance of their networks and supply information to state investigators on request, in addition to having their equipment reviewed for security. They are also required to censor prohibited content and to reduce user anonymity by requiring real-name registration."[15] This means companies are compliant with the development of a "Social Credit System" that would "assess the conduct of every person in the country."[16] Yet, Congress cannot see this cooperation and use of individual data under blanketed user agreements that must be accepted for access to technology as forming behavioral instrumentarian power on their own soil. Orwellian behavior is nonetheless creeping into the United States' own

[14] H.R. Rep. No." Hearing Before the Subcommittee on Asia." 2.
[15] Qiang, "The Road to Digital Unfreedom." 55. This is discussed in Chapter 3.
[16] Ibid. 54

systems unregulated. Law enforcement in the United States is working with corporations like ClearView AI. A company not unlike China's Sky Net.[17] In addition information on users is being stored by all of the big data companies in data-warehouses to create "seamless" user experiences. In reality this is done to create micro-target advertisements for users across social media platforms and the internet. Thus, while business and government are thought to be separated in the United States, it is becoming increasingly clear there are connections between the government and corporations in regard to data obtained for surveillance capitalism.

As can be seen, a great deal of analysis has been conducted on the cause of the shift in technological alignment with democratic values to that of authoritarian tendencies. There has also been research done on the consequences of this shift. However, more research is needed on the consensus and complicity of the United States in this process as well as its cooperation with China in the form of corporations. Democratic values exported by regimes of the same name in the initial invention of the internet have been diluted by private business interests under the guise of state security and state sovereignty in a world where international relations and hegemonic power dynamics have moved from the real world to cyberspace. Authoritarian regimes like China have never kept their desire to monitor and control civilian actions a secret. However, their ability to do so on a massive scale is increasing with the new technology. This opportunity is not lost on democratic societies. Thus, this study addresses the increasing influence that state surveillance and surveillance capitalism have on the structure of the legal and political systems in the United States and the impact that these changes have had on already vulnerable populaces. China's use of surveillance technology will serve as a counterexample to show how quickly the use of this technology can shift from democratic to authoritarian uses. This analysis cannot fully

[17] Hill, "The Secretive Company That Might End Privacy as We Know It."

illustrate the global implications of the use of this technology but hopes to encourage more research on this area after illustrating how the United States and China are exporting these systems.

In order to examine the increased use of these technologies by two different regimes, a descriptive qualitative comparative analysis is conducted. While the development of these technologies has had different ebbs and flows regionally throughout history, the period being studied focuses on the use of this technology just prior to September 11th to present day. This illustrates the profound shift 9/11 had on the trajectory of surveillance in the United States and show how similar events are being used in China to justify increased surveillance. The attacks on the Twin Towers had a global impact that made all heads of state reevaluate their ability to prevent a similar situation in their own countries. The increase in ethnic rioting in China in 2009 was the culmination of tension between the Uyghur population and Han Chinese. This relationship has many historical causations and is a complex issue that will not be dissected in this analysis. However, the focus on religious differences between these two groups is a tactic used by the Chinese government. Thus, this assessment of the conflict is taken as an indication of the government's attempt to link organizations involved with the September 11th attacks to conflicts on their own soil.

This research is conducted through examining the development and deployment of United States and Chinese surveillance technology while also investigating the efficacy of the security programs. This information has its limits as the NSA and other governmental agencies in charge of national security do not make their records public nor can they comb through the entirety of the data that their programs collect due to the nature of bulk data collections. The corporations that gather user information even under the new California Data Protection Law passed this year, make it exceedingly difficult to analyze the information stored on users, even if they have the technological literacy to request this information through the proper channels. Additionally, the Chinese government is notorious for the limited amount of information they allow to be exported. However, this thesis analyzes specific cases that illustrate the use of this technology and its impact on civilians in the United States and China to mitigate the inefficacy of security reports. Most of the evidence is qualitative in nature due to differences in data collection and their complex nature. As much of this data is provided by states or state organizations, most sources are secondary. The analysis conducted from these sources is done with the understanding each of these sources are not immune to corporate and political biases of the organizations that collect and present the information. Furthermore, each of the sources is vetted for credibility to ensure this evaluation can be conducted as impartially as is possible. This is by considering the missions and affiliations of those producing the information. This comparison and analysis is being done to supplement future research conducted on the implication of the exportation and utilization of this technology regardless of regime type on civil rights and to encourage the adoption of laws and policies dedicated to the restoration of the balance of power between civilians and corporations.

Chapter 1: Technology, Security, and the New Environments They Create

As technology is a vast field in which specific jargon is utilized, there are certain words that need defining before analyzing their interaction with civil society in different regimes. To begin, let us examine surveillance technologies. This technology is often used to increase state security. Security, in this context, is referred to as the means through which a state protects its populace. While many countries felt the ability to maintain a secure state in a globalized world was already challenging, post-9/11 countries relied on “post-World War II notions of security, in which guarantees of inviolability and protections are sought by technical and military means as political goals.”[18] Thus, security in the modern world relies heavily on surveillance. Broadly, surveillance means “to watch over.”[19] Surveillance technologies can include several types of information technologies. Usually they are built by combining hardware with the “internet of things” to provide organizations with the ability to “watch over” what activities are being conducted. The internet of things is the network of physical objects connected to the internet through sensors, software, and other means. Eric Schmidt, Google’s CEO until 2011 described it as when “The internet will disappear. There will be so many IP addresses…so many devices, sensors, things that you are wearing, things that you are interacting with that you won’t even sense it. It will be a part of the presence all the time.”[20] The creation of this system enables bulk data interception through Information Communication Technology (ICT) and monitoring abilities through the internet, wireless networks, cell phones and computers. Geo-location or remote sensing of where individuals go and who they go there with can be found through these tools. Biometric identification is another form of surveillance technology. This type includes the

[18] Lyon, *Surveillance after September 11,* 15.
[19] Ibid.
[20] Zuboff, *Surveillance Capitalism,* 199.

use of fingerprints, facial features, and irises collected through photographs or video monitoring.[21] Heart rate and oxygen levels if combined with a device such an Apple Watch or Fitbit can also be included in this category.

Another tool used by those looking to surveil is internet content filtering.[22] This is defined as "techniques by which control is imposed on access to information on the internet." This can take the form of address blocking (such as blocking entire websites that use particular internet protocol or IP addresses) or content analysis (which blocks particular information such as keywords or specific URLs).[23] Without getting bogged down in the nitty gritty of how the "internet" works all that must be understood is that the internet is like a set of train tracks and the world wide web is like the train that allows the information to be carried in a neat package to be received at the destination. However, along the route there are different "gateways-from routers to IXPs (internet providers) to autonomous systems-present opportunities for authorities to impose order on internet traffic through some mechanism of filtering and surveillance…[some] takes place for technological reasons; some of it takes place for cultural political, and economic reasons."[24] Many of these tools are now being amplified by artificial intelligence (AI) and machine learning. In her book *Artificial Unintelligence: How Computers Misunderstand the World,* Meredith Broussard demonstrates that as the term "machine learning" is relatively new, there is not a consistent definition. Like her, I find the most accurate definition is given by Tom M. Mitchell, a professor at Carnegie Mellon University's School of Computer Science. He defines it by stating, "We say that a machine learns with respect to a particular task. T, performance metric P, and type of experience E, if the system reliably improves its

[21] Ünver, "Politics of Digital Surveillance," 7.

[22] A method that will be discussed in relation to China in Chapter 3.

[23]Andrew et al.,*"The Geopolitics of Internet Control Censorship, Sovereignty, and Cyberspace."* 325.

[24] Ibid. 324

performance P at task T, following experience E. Depending on how we specify T, P and E, the learning tasks might also be called by names such as data mining autonomous discovery, database, updating, programming by example, etc."[25] As Broussard illustrates in her book, artificial intelligence and machine learning, "doesn't mean the machine has a brain made out of metal. It means that the machine has become more accurate at performing a single, specific task according to a specific metric that a person has defined, this kind of learning does not imply intelligence."[26] Thus, artificial intelligence does not mean that machines have been given the ability to think autonomously, it simply means they can improve tasks with parameters set by humans. As Broussard states, "If I could beat a Grandmaster at chess and yet not be able to hand you the salt at the table when asked, would I be intelligent?"[27] However, this "intelligence" does mean that tasks can be given to a machine on a massive scale, and the machine, if programmed correctly, can sort the information, write a journal article, etc. One example is IBM's Artificial Intelligence computer named Watson. It was programmed to scan medical journals to help treat cancer patients. However, some advice given by the machine could have made patients worse. For instance, medication that could increase bleeding was suggested for patients with severe bleeding.[28] This last concept comes into play later in the thesis when discussing the impacts of information technology on social groups.[29]

Now that the technology being analyzed and the language used to describe it have been clarified, the environments in which they are deployed must be defined. Two such environments have become the focus of the Department of Justice. These are "information power" and the

[25] Broussard, *Artificial unintelligence: How computers misunderstand the world,* 99.
[26] Ibid.
[27] Ibid.
[28] Chen, "IBM's Watson Gave Unsafe Recommendations for Treating Cancer."
[29] See page 50.

"information environment." The DOD defines the Information Environment (IE) as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The IE is a heterogeneous global environment where humans and automated systems observe, orient, decide, and act on data, information, and knowledge. With its function as a conduit for influence on decision-making and command and control…Characterized by ubiquitous on-demand media and interpersonal hyper-connectivity, today's IE enables collaboration and information sharing on an unprecedented scale."[30] This, they believe, leads to "an impact in the human cognitive dimension making it the central object of operations in the IE."[31] Ultimately, this information can be harnessed as what they call information power. They define this as, "The ability to leverage information to shape the perceptions, attitudes, and other elements that drive desired behaviors and the course of events. This includes the ability to use information to affect the observations, perceptions, decisions, and behaviors of relevant actors; ability to protect and ensure the observations, perceptions, decisions, and behaviors of the Joint Force; and the ability to acquire, process, distribute, and employ data (information)."[32] The Department of Defense's focus on these areas is in an effort to "incorporate the concept of the preeminent nature of information into the design of all operations to maximize military power."[33]

These definitions and concepts put forth by the DoD are almost identical to those analyzed by Julie E. Cohen, Michael Castell and Shoshana Zuboff when discussing surveillance capitalism and information power held by the corporate sector. To further illustrate the connection of surveillance capitalism and information power to the information environment and

[30] Department of Defense. (2016). *STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT* (pp. 2-15, Rep.). Washington, D.C: Department of Defense, 3.
[31] Ibid.
[32] Department of Defense. (2018). *Joint Concept for Operating in the Information Environment (JCOIE)* (Rep.). Washington, D.C: Department of Defense. viii
[33] Ibid.

information power identified by the DoD and its ubiquitous nature and impact on "human cognitive dimension[s]," the definition at the start of Zuboff's book warrants its full quotation. She presents the definition as:

> "**1.** A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales; **2.** A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioral modification; **3.** A rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history; **4.** The foundational framework of a surveillance economy; **5.** As significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth; **6.** The origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy; **7.** A movement that aims to impose a new collective order based on total certainty; **8.** An expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty."[34]

Julie E. Cohen uses Michael Castell's define information capitalism as, "the alignment of capitalism as a mode of production with informationalism as a mode of development."[35] To further dissect this concept she clarifies capitalism and informationalism as follows, "Capitalism 'is oriented toward profit- maximizing, that is, toward increasing the amount of surplus appropriated by capital on the basis of the private control over the means of production and circulation,' while informationalism 'is oriented . . . toward the accumulation of knowledge and

[34] Zuboff, *Surveillance Capitalism,* 10.
[35] Cohen, *Between Truth and Power,* 5-6.

towards higher levels of complexity in information processing.'"[36] Between the state and private sectors, collection and utilization of data has many names. However, the use of this data has one goal: influence and control on cognition and societal behaviors. Thus, whether referring to the information environment, information power, surveillance capitalism, instrumentarian power, or information capitalism throughout this thesis, the connection between user generated data and power over societies actions should be front of mind when hearing these terms.

As this thesis attempts to determine the role of regime type in the use of this technology, differences between these regime types should be made clear. The difference between authoritarian and democratic regimes has historically depended on the participation of the populace in political decisions and the electing of officials as well as the freedoms of the people within the territory. According to Juan Linz, the definition of democracy means individuals have "legal freedom to formulate and advocate political alternatives with the concomitant rights to free association, free speech, and other basic freedoms of person; free and nonviolent competition among leaders with periodic validation of their claim to rule; inclusion of all effective political offices in the democratic process; and provision for the participation of all members of the political community, whatever their political preference."[37] While this definition of democratic regime is applicable to this research, it needs to be noted that "free speech," "free association" and "other basic freedoms of person" are being interpreted as having a certain amount of privacy, self-determination, and cognitive liberty associated with them. As far back as the 1970s a subcommittee on Constitutional Rights had been formed after the CIA began to focus on behavioral-modification research. This research was dedicated to understanding the

[36] Ibid.
[37] Linz, *Crisis and Breakdown*. 5

"Chinese brainwashing techniques, reinterpreting them through the established frameworks of behavior modification." [38] The research concluded, "'human material was changeable'—that one's personality, identity, awareness, and capacity for self-determining behavior could be crushed, eliminated, and replaced by external control."[39] Senator Ervin stated in the subcommittee's 1974 report "When the founding fathers established our constitutional system of government, they based it on their fundamental belief in the sanctity of the individual…They understood that self-determination is the source of individuality, and individuality is the mainstay of freedom…Recently, however, technology has begun to develop new methods of behavior control capable of altering not just an individual's actions but his very personality and manner of thinking…[this] touches upon the most basic sources of individuality and the very core of personal freedom."[40] Privacy will be defined as it relates to the Fourth Amendment to the United States Constitution. This amendment declares "The *right* of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[41] Barry Friedman and Orin Kerr, professors of law at NYU and George Washington University respectively, in their "common interpretation" of this amendment admit that the technologies discussed above have made the interpretation of this amendment more complex and vital to the conversation of what constitutes a "search" and whether "cause" is even considered. In their collective analysis they ask whether information given to internet providers or other third parties if used by the government constitutes a "search." In terms of cause, they give the example

[38] Zuboff, *Surveillance Capitalism,* 323.
[39] Zuboff, *Surveillance Capitalism,* 321.
[40] Ibid, 324.
[41] U.S. Const. Art. 4

of being searched at the airport. No one has been accused of doing something wrong and yet everyone knows upon entering they will be searched. They liken this to the collection of bulk data and potentially the use of biometric information gathered through surveillance technology.[42] They do not--in this interpretation--state whether any of these new questions presented by technology have answers in relation to this amendment. Thus, the newly passed California Consumer Privacy Act (CCPA) or "AB 375" enforced as of January 1, 2020 and Europe's GDPR will act as the litmus test to what democracies feel constitutes the right to privacy in terms of data. As the Hastings International Comparative Law Review states, "The right to privacy is a fundamental human right enshrined in the Universal Declaration of Human Rights, The European Convention on Human Rights, and the European Charter of Fundamental Rights."[43] Therefore, these new legislative acts extend these to data protection in the following ways, "(1) limits on the collection of personal data; (2) transparency in collection and processing; (3) substantive rights for individuals subject to data collection; and (4) enforcement and accountability."[44] Categories that align with the definition of democracy put forth by Juan Linz.

How to determine whether a democracy is under siege is a complicated subject that many books published after the U.S. 2016 presidential election have been brave enough to undertake. While the goal of this analysis is not to determine whether the entire institution of democracy is at stake in the United States, defining how this technology is being used compared to China's authoritarian regime is an allusion to the threat the system is facing because of these newfound technologies and the means through which they are being deployed. Shoshana Zuboff illustrates in her book the relationship between social trust and civic engagement. She states, "In its

[42] Friedman and Kerr, "The Fourth Amendment." 1

[43] Heward-Mills and Turku, "California and the European Union Take the Lead in Data Protection," 319.

[44] Ibid, 321.

absence the authority of shared values and mutual obligations slips away…Confusion uncertainty, and distrust enable power to fill the social void."[45] She states that surveillance capitalism and the instrumentarian power of corporations fills the void.[46] I would add that the Department of Defense references to the information environment and information power and the efforts of the Chinese government to create a "Social Credit" system show that the state is also seeking to take advantage of the uncertainty and distrust in the governing institutions by society through the technologies being utilized. As a prediction of this trend she shows the percentage of Americans said they had trust in the government "most or all the time."[47] In 1985 this number was at 75%, in 2017 it was at 18%.[48] This analysis uses the inability of well-educated lawyers like Barry Friedman and Orin Kerr to determine whether the Fourth Amendment holds merit in the technological realm and the work of Juan Lintz, Steven Levitsky and Daniel Ziblatt on what elements threaten a democracy to determine whether this technology is being used in a way the definition of democracy would denote. A modified version of the metrics created by Ziblatt and Levitsky based on Juan Lintz's work are applied to conduct this analysis. They apply these parameters to politicians. However, for the purposes of this thesis these are extended to the state and corporations in the United States and China. Thus, the modified metrics include:

1) The rejection "in words or action" of democratic norms.
2) The denial of the legitimacy of alternative choices
3) "Tolerates or encourages violence."

[45] Zuboff, *Surveillance Capitalism, 383.*
[46] Zuboff, *Surveillance Capitalism, 383.*
[47] Ibid.
[48] Ibid.

4) “Indicates a willingness to curtail the civil liberties of opponents including media.”[49]

China will act as the base variable for an authoritarian regime as its creation, use and distribution of this technology is on par with the United States. Thus, the similarities and differences of the United States to China in these categories is the basis for the conclusion to the following hypothesis.

Hypothesis: While the type of political rule created vastly different types of information technology when the internet was first created, the pressure international terrorism put on state security concerns and the use of surveillance capitalism by corporations have been compounded by the lack of transparency in their use. The result is that the gap between information technology in authoritarian and democratic governments has diminished over time.

One last concept must be clarified before this hypothesis can be fully examined, namely, that of an autocracy. An autocracy is typically defined as a system of government by one person with complete power and usually has either a dictator or monarchic figure in control. According to a study produced by the Center for European Studies at the University of Texas at Austin, China is classified as a one-party authoritarian regime where there is “generally an elected legislature where only one party is represented.[50] While some have argued that China does not fall under the category of authoritarian regime because of the popularity of the government, it is still commonly accepted that China is in fact an authoritarian dictatorship, albeit a popular one. Due to this popularity, the type of autocracy this analysis uses for China is a “soft authoritarianism whereby collective well-being is more important than individual liberties and

[49] Levitsky and Ziblatt, *How Democracies Die*, 21-22.

[50] Wahman et al., “Authoritarian regime types revisited: updated data in comparative perspective,” 19–34.

national development is more important than political rights."[51] Due to the nature of this regime, business practices and government in China are inextricably linked. Thus, while separate attention is paid to both corporations and the state in the case of the United States, China's situation is analyzed understanding that business and the government are not separated in the same way.

Both the United States and China are world powers. Historically, these two countries are often on different sides of human rights issues and political ideologies. Could the combination of increased non-state actor terrorism and the enhanced development of surveillance technologies lead these two countries on a convergent trajectory? Or will the different political structures of these countries keep the use of this technology from overlapping?

[51] Gueorguiev, "Mike Bloomberg said China isn't a dictatorship. Is he right?"

Chapter 2: Historical Orientation of State Surveillance and Human Rights

The state has always been at the forefront of surveillance for the purpose of security. The degree to which the state has access to private information has typically depended on the regime type. Democracies tend to rely on due process to collect personal information. In contrast, in authoritarian regimes such as China, the culture of putting the good of the whole before that of the individual has meant that privacy is not seen as a right if it interferes with the goals of the state. In a popular dictatorship, this is swayed by public opinion but not controlled by it. Security and surveillance are not inherently negative attributes of a society. Cameras are places in stores, homes, and even in police interrogation rooms. These are not there to harm but to ensure social norms are adhered to. They prevent theft and violence. They provide security. However, after 9/11 these systems were amplified exponentially. Before looking at the after-effects it is imperative to understand the historical context technology was introduced into the United States and China.

Privacy has always been a priority of the United States democratic rulers. A clear example of this can be seen in the legal battle over the 1986 Immigration Reform and Control Act. This was initially supposed to deter the inflow of new illegal immigrants. However, even conservatives, who traditionally are in favor of stronger measures of control to achieve national security measures were against the employment verification system that was later called the “national ID card” that was part of the legislation. A conservative journalist wrote in the *New York Times*, “it is better to tolerate the illegal movement of aliens and even criminals than to tolerate the constant surveillance of the free."[52] While this example deals with immigration. it is an important instance of the fundamental beliefs of the United States before 9/11.

These beliefs transformed into the ideologies that were prominent when the internet was being created. Upon its founding the utopian intentions clouded the control mechanism that dominated the infrastructure. Tim-Berners Lee, who founded the World Wide Web, wanted to create an egalitarian platform for information sharing. What many do not know is that, before the internet was accessible on personal computers, ARPAnet was the first network to use this form of "packet-switching" or information carrying from one closed computer network to another. ARPA was the Advanced Research Projects Agency of the Department of Defense in 1969. It was created to hold information on multiple channels to assure there would be safeguards in place in case of a nuclear attack. This technology reached individual households through the proliferation of personal computers. Free speech, anonymity, decentralized ownership, open infrastructure, and permission-less innovation all guided the early years of the internet and the World Wide Web.[53] The economics of the system were not the focus. Information and liberty were the commodities.

The People's Republic of China has existed since October 1949. Long before this system was in place. Thus, the cultural parameters in which the internet was introduced to China are imperative to understanding its relationship with this technology. Society and technology are thus, inextricably linked. As Manuel Castells states, "Mainly by state intervention, [technology] can embark on an accelerated process of technological modernization able to change the fate of economies, military power and social well-being in a few years."[54] In other words, it is a tool of

[52] Joppke, "Why Liberal States Accept Unwanted Immigration," 274.
[53] Brandom, "We Have Abandoned Every Principle of the Free and Open Internet."
[54] Castells, *The Rise of the Network Society*, 7.

the society in which it operates. While the priority in the United States leaned towards freedom of expression and liberty, China's had a more complicated relationship with this new technology. It saw the internet as an entity of "Western" influence. A piece in the *Global Times*, a state-run newspaper in China "accused the United States of using the notion of an unrestricted Internet as a disguised imposition of its values on other cultures…information imperialism"[55] In a communist culture, often at odds with the United States, this sentiment is understandable. However, its economic advantages could not be ignored and in 1980 under Deng Xiaoping, the leader of the People's Republic of China from 1978 to 1989 the information communication technology (ICT) sector became more pronounced.[56] Thus the state had to balance the impact of an entity that was created to spread information in an atmosphere where control of information was thought to be necessary to protect the needs of the collective while also incorporating some of these new technologies to keep up with a globalizing world. State prosperity and its global position would be compromised had China not adopted this technology.

In the world pre-September 11th, the internet posed fewer challenges to state control. Democratic countries mainly had to worry about inappropriate content while authoritarian regimes had to manage what was deemed appropriate for public consumption while wrestling with what impact this "western" influence would have on their way of life. Neither regime was totally without concerns. In other words, "All countries face political challenges from the internet. Democracies are not immune and face immediate problems, but in the long term, information technology poses the greatest challenge to authoritarian regimes. Information technologies create an existential threat for authoritarian regimes that they are hard pressed to

[55] Open Net Initiative, "China."
[56] Ibid.

manage. Authoritarian regimes, with their brittle relationship with their own citizens, have reacted by trying to suppress this political effect by restricting access to information, providing counternarratives for both domestic and foreign consumption, and by creating ubiquitous surveillance."[57]

While the sentiment of the above quote still rings true, the impacts of September 11th and other terror attacks combined with the arrival of a global pandemic have been compounded by the involvement of corporations in this process. Altruistic intentions of governments are being replaced by monetary considerations that have been strengthened by these global security threats. This has in turn reinforced the state's interest in information power as defined by the Department of Defense. The following chapters further investigate the relationship of information technology and citizens of democracies and authoritarian regimes after the influence of terrorist attacks. The role of corporations in this process are analyzed as well in subsequent chapters.

[57] Lewis, "Cognitive Effect and State Conflict in Cyberspace," 3.

Chapter 3: China's Increasing Surveillance and its Impacts on the Marginalized

China and its businesses have historically been interconnected. With the implementation of the Belt and Road initiative, the focus on technology and surveillance is increasing locally and internationally. China's thought process that cyberspace is a territory dominated by "Western" influence consumes the relationship between the government and technology. In China, large corporations work closely with the government to create "Safe Cities" and a "Social Credit System." While the reasons for these partnerships vary, massive amounts of personal data are being collected and used to establish a "rule of trust" instead of a "rule of law." These systems are targeted towards already marginalized populations. Furthermore, the technologies that are being created in China are being exported globally. Therefore, their proliferation could lead to a potential international human rights issue. This chapter looks at the connection of surveillance by the state and businesses in China to illustrate the consequences of a pervasive surveillance system on daily life when utilized by the government and corporations without regulation.

As mentioned above, China's relationship with the "western" infrastructure under an authoritarian regime has meant that internet content filtering is not a new tool for the government.[58] This has often come under United States scrutiny. Secretary of State Hillary Clinton in 2010 criticized the country for compromising the open flow of information. In response, the Global Times, a newspaper controlled by the Chinese Communist Party accused the U.S. of "using the notion of an unrestricted Internet as a disguised imposition of its values on other cultures-in other words, information imperialism."[59] Some content is stopped at the router level making it impossible for a computer's IP address from accessing information deemed inappropriate initially while also preventing that address from making similar requests for a

[58] See page 12 for information on how this tool works.
[59] Open Net Initiative, "China."

certain amount of time. Other methods include blocking URL addresses and keywords from being visited or searched from within China.[60] Many identify this as the "Great Firewall of China." The *Global Times* supported these tactics by stating "countries disadvantaged by the unequal and undemocratic information flow have to protect their national interest and take steps toward this. This is essential for their political stability as well as normal conduct of economic and social life."[61] The Chinese Foreign Ministry site also quoted Ma Zhou, a spokesperson for the government, who stated, "we urge the U.S. to respect facts and stop attacking China under the excuse of the so-called freedom of the Internet."[62] While this statement is a clear indicator of the current Chinese government's views on the internet, they have not always had as strict a position. In 1994 it was a portal to Western information and a tool for opening the economy. However, as its use increased in the country, it began to come under further restrictions culminating in the establishment of the "Great Firewall" in 2000. This was combined with a project called the "Golden Shield" which worked with China's security forces to create a surveillance system driven by data. This system targeted citizen's records. The focus on China's "cyber sovereignty" has been further increased under President Xi Jinping. Now over 50,000 staff members of the government have been made responsible for this censorship. Companies who wish to access Chinese markets must respect the decision of the administration creating backdoors into users' profiles as well as allowing the data gathered through products to be stored in China for easier access by the Chinese government.[63]This censorship and surveillance have

[60] Andrew et al., "The Geopolitics of Internet Control Censorship, Sovereignty, and Cyberspace." 324
[61] Open Net Initiative. "China."
[62] Ibid.
[63] Chan, "The Great Firewall of China."

increased exponentially in provinces such as Xinjian where the concentration of the Uyghur population is the most concentrated.

According to an article by the Wall Street Journal, “China’s Central Asia frontier may be one of the most closely surveilled places on earth.”[64] After the ethnic riots in 2009 in Erdaoqiao that resulted in several deaths, the Mosque and religious shops were closed in the region. This was escalated by terrorist attacks in 2014 that China blames on militants in Xinjiang influenced by Islamic extremists abroad. These attacks, much like the terrorist attacks that took place on September 11th, have resulted in increases in surveillance in the area and across the country. With improved technology and efforts targeted on enhancing systems put in place, a ubiquitous surveillance system has been created. I.D cards must be swiped for routine transactions such as filling a car with gas or when going to the mall. Police now use handheld scanners to search the contents of smartphones for items like chat applications that use encryption. A plethora of cameras scan faces, retinas, and at times entire bodies. Cars are stopped when crossing regional borders. License plate cameras and location trackers placed in all commercial vehicles make spotting visitors easy. Chen Quanguo the Xinjiang party chief appointed recently by Xi Jinping has increased police presence and is responsible for the use of cameras capable of creating DNA sequencers, 3-D face images, and analyzing voice patterns. Companies such as China Telecom and Xiamen Meiya Pico Information have received contracts worth millions to increase surveillance in the region and improve the scanning devices used on smartphones.[65] The *Global Times* likens its use of surveillance technology in this region to “a similar trend…in the US and Britain for the purpose of fighting terrorism.”[66] The piece claims “About 95-98 percent of

[64] Chin et al., “Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life.”
[65] Chin et al., “Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life.”
[66] Global Times “Surveillance tech grows in Xinjiang, necessary to counter terrorism.”

terrorist activities can be stifled in their nascent period."[67] Operation "Xue Liang" or "Sharp Eyes" taken from the Communist phrase "the masses have sharp eyes," is not restricted to this region.[68]

The anti-extradition bill protests in 2019 in Hong Kong show another minority targeted by these surveillance systems. Protests broke out as the Anti-Extradition Law Amendment Bill would have allowed local authorities to extradite fugitives that were wanted outside of Hong Kong. Citizens were afraid this legislation would hamper the region's independence and civil freedoms due to the ability to extradite citizens to mainland China.[69] Hong Kong protesters faced digital surveillance from authorities. In Hong Kong protesters refused to use subway cards linked to their identities and security cameras were either smashed or disrupted by laser pointers. Face masks were also worn to prevent detection (this took place pre-COVID 19). Protesters also stopped using credit cards or driving their cars to protests due to a fear of being recognized by license plate scanners.[70] The cooperation between Hong Kong police and mainland China as well as similar surveillance technology worried the protesters. This is not unwarranted as Hong Kong sends about 150 officials to China each year for training from police academies. However, it was still possible in Hong Kong for protesters to install VPNs on their devices and communicate through a secure messaging app called Telegram. Protesters were able to share information about how to avoid detection using pay as you go sim cards and changing the number associated with the encrypted chat. Many warned against taking pictures during the protest so as not to be targeted on social media accounts.[71] In a hearing conducted by the House of Representatives

[67] Ibid.
[68] Deneyer, "China's Watchful Eye."
[69] Caffrey, "2019 Hong Kong Anti-Extradition Bill Protests."
[70] Ovide, "The Real Dangers of Surveillance."
[71] Mahtani "Masks, Cash and Apps: How Hong Kong's Protesters Find Ways to Outwit the Surveillance State."

subcommittee on Asia the Pacific and Nonproliferation, in the U.S., protesters were included with a representative from Human Rights Watch and a Uyghur who had been through the "re-education camps" in China.[72] In the report, House spoke out against the "Orwellian Surveillance State" and the "digital authoritarianism" being used in China.[73] However, as is discussed in the following chapters on the U.S., the systems used to target these individuals are not vastly different than those being developed in the United States.

This technology is being used across China in various ways. Facial recognition is used to unlock resident apartments, by customers at bank ATMs, when users "beautify "themselves with phone applications, and at restaurants such as Kentucky Fried Chicken where a customer can purchase items through their "smile to pay" system.[74] All of this is in an effort to create a "Social Credit System" and create a predictive crime system. China's system is said to be effective enough to scan the population of China in one second and the world's population in two. China had released information previously stating their goal was to have 570 million cameras in the country by this year. That would equate to one camera for every two citizens.[75] The "Police Cloud," or Integrated Joint Operations Platform also goes by the name "Sky Net." This system collects information such as whether someone's phone is off for an extended period of time, if they use the back door or the front door, where people have been, who they have been associating with, delivery records, and medical histories. This information is shared across a number of platforms. It is aggregated with information pulled from government organizations, police data, and company data. This can include information from telecom companies, internet

[72] H.R. Rep. No., "Hearing Before the Subcommittee On Asia," 13.
[73] Ibid.
[74] Deneyer, "China's Watchful Eye."
[75] Chan, "16 Parts of China Are Now Using Skynet, the Facial Recognition Tech That Can Scan the Country's Entire Population in a Second."

blogs, and social media accounts. Some information is also purchased from third-party companies which give information such as search data on the internet and purchases from e-commerce companies[76] By using artificial intelligence, this program can also alert police to behaviors it deems as unusual, such as someone staying in a hotel they know to be a resident locally. It is also anticipated this system will be able to identify relationships authorities would not otherwise recognize. Specific groups are made priorities, such as those that have been involved with crimes, drugs, and those who have mental health issues or who "tend to cause disturbances."[77] This system and its predictive capabilities are limited at the moment for a number of reasons. These include but are not limited to, incomplete information, inconsistent information, and the skills of those meant to utilize the system. Once these are improved, however, the surveillance possibilities are endless as there are few laws that require the police to obtain court orders to conduct surveillance, they deem necessary. Instead, these practices are being incorporated into China's legal system and are being used to create a "rule of trust."

In June of 2017, The Intelligence Law was passed by the National People's Congress. This "makes explicit what has long been done in practice."[78] There are also State Security Laws and Cybersecurity Laws incorporated into the system that allows massive amounts of information to be collected and stored within the Chinese territory.[79] The social credit system is pushing the country away from the claims of "governing the country in accordance with the law" and forming instead a "rule of trust" whose definition is frequently changing and directly undermines the "rule of law."[80] The Chinese government's use of "trust" enables them to justify intrusive

[76] Human Rights Watch, "China: Police 'Big Data' Systems Violate Privacy, Target Dissent."
[77] Ibid.
[78] Canadian Security Intelligence. "Government of Canada."
[79] Human Rights Watch, "China: Police 'Big Data' Systems Violate Privacy, Target Dissent."
[80] Chen at al., "Rule of Trust: The Power and Perils of China's Social Credit," 3-6.

technologies like those described above and the discrimination against those deemed as "trust-breakers" such as those in the Xingjian province categorized as such because of their ethnic or religious connections to those the government deems troublesome. While the Chinese Social Credit System does not yet give the citizens a universal score, companies such as Ant Financials' Sesame Credit use cloud systems and machine learning to give users a score. The Chinese government is also using the system to further aggregate credit information collected across platforms into a "National Credit Information Sharing Platform."[81] This system includes departments designed to service the people such as, tax, police, civil affairs, environment treasury, finance, customs agencies, etc. totaling 37 ministries. This system is to distribute both rewards and sanctions to those the government decides are keeping the trust or breaking it, respectively.[82] Those in the Xinjiang province are not the only ones being micro-targeted by such systems.

The uses of these technologies are permeating cities abroad as well. This can be seen in the creation of Huawei's "Safe City." China is now considered a major technological developer and supplier of technologies abroad. Huawei, a Chinese company, is a major factor in this global adoption of technologies. It offers cheaper products that U.S. companies like Apple and Google make with very similar capabilities. They also export goods such as cameras and monitors. China's Belt and Road Initiative have made this global exchange of goods a priority. Over 197 cooperation documents were signed with 137 countries and 30 international organizations in October of 2019. The trade between January and September with these countries totaled approximately 950 billion U.S. dollars and its "non-financial direct investment in these countries

[81] Ibid, 12-17.
[82] Ibid, 3-6.

topped 10 billion dollars."[83] Huawei in its 2018 end of year report wrote, "Our cloud business needs to further develop its AI capabilities and hone its competitive edge in enterprise services. It needs to establish a stronger presence in e-government, automotive ICT components, and safe city domains, and maintain high-speed growth with healthy gross margins."[84] It describes a "Safe City" as using ICT technologies such as AI, cloud computing, the internet of things, and big data. It mentions having exported these technologies to over 700 cities in 100 countries. These regions include places like Brazil, Mexico, Serbia, South Africa, Turkey, Spain, and Singapore.[85] Other companies, such as Cloudwalk, are following closely behind with the *Global Times* reporting exportation of facial recognition to Zimbabwe in 2018 as part of the Belt and Road initiative.[86] Therefore, China's use of surveillance technology is not only becoming ubiquitous in the region but is proving internationally relevant through its Belt and Road initiatives and focus on making technology a connecting factor between countries.

As the counterexample to the U.S., it is clear that the parameters put in place to determine if democratic processes are being followed do not apply to China. There are no limits or transparency in the data collection process. The rights of individuals regarding the use of their data does not appear to be relevant. No alternative choices can be made as to how users' interactions with technology are monitored. A simple internet search that is deemed inappropriate could gain an individual negative marks on their "social credit" score. Taking the backdoor instead of the front out of the house could result in being classified by authorities as someone to be watched by the predictive crime system. Minority groups are especially impacted. This takes place in the form of "re-education camps" and the classification of opponents to the

[83] Xinhuanet. "China Signs 197 B&R Cooperation Documents with 137 Countries, 30 Int'l Organizations."
[84] Huawei Investment & Holding Co. Ltd. 2018 Annual Report, 6.
[85] Ibid.
[86] Jie, Shan. "China Exports Facial ID Technology to Zimbabwe," 2018.

government such as the Hong Kong protestors as subversives. These categorizations can hurt individuals' chances of getting a loan or leaving the country.[87] Such labels could also result in direct violence due to the cultural tension between different ethnic groups.

The following chapter evaluates similar cases of surveillance in the United States. It focuses on the substantial shift that occurred in how surveillance was used pre-9/11 to post-9/11. By using the same parameters of how data should be protected in a democracy and focusing on the metrics laid out on page sixteen, the chapter analyzes the use of this technology in the United States to determine if our democracy is strong enough with enough systems in place to prevent Orwellian tendencies to become a norm in America as they have in China.

[87] The parameters around practices detrimental to democracy can be found on page 19. Page 17 contains references to data protections that should be found under a democracy.

Chapter 4: State of Emergency and the New Normal-State Control

September 11th prompted an unprecedented crackdown on surveillance in the United States. The state felt it needed to pivot to protect its populace. Thus, the Patriot Act was passed a mere 6 weeks after the event on October 26, 2001. The legislation was over 300 pages in length and therefore, was not read in its entirety by representatives. Therefore, it is unsurprising that some of the consequences of this shift in legal framework had unintended consequences. Trying to track decentralized terrorist organizations meant that the Fourth Amendment and civilian privacy concerns took a backseat to the collection of information.[88] The Patriot Act along with the Terrorist Screening Program not only lead to the collection of information on foreigners in the United States, these programs also increased warrantless collection of personal information of the citizenry.

David Lyon describes the quick 180-degree shift from a consumer focus to security in his book, *Surveillance after September 11th*. The Federal Trade Commission before the attacks had already realized that the self-regulation of technological companies was not going to be sufficient for protecting consumer rights. One year before the attacks, the majority of the FTC commissioners recommended a change to the laws that would regulate privacy. In a report they concluded, "Because self-regulatory initiatives to date fall short of broad-based implementation of self-regulatory programs the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders."[89] They called for "'clear and conspicuous" notice of information practices; consumer choice over how personal information is used; access to all personal information including rights to correct or

[88] McAdams, "Internet Surveillance after September 11."
[89] Zuboff, *Surveillance Capitalism 118*

delete; and enhanced security of personal information."[90] This focus on protecting consumer rights faded after 9/11. Peter Swire, the Chief Counselor for Privacy in the Clinton Administration and a member of the Review Group on Intelligence and Communication Technologies under Obama said, "With the attacks of September 11,2001 everything changed. The new focus was overwhelmingly on security rather than privacy."[91] Lyon also explains how the speed at which this act was passed left little room for debate. He attributes the emotion evoked from the nature of the attack to a lack of scrutiny of the bill by those passing it into law. Due to the lack of understanding by representatives of its complexities it was impossible for the citizenry to realize its reach. Thus, he states, "Not only is a culture of suspicion emerging, but a culture of secrecy is also emerging alongside it."[92] As previously mentioned, this has become detrimental to civil participation due to a lack of trust in the government.

The nature of the information collected also made it difficult to uphold previous privacy promises. Emails and Call Detail Records (CDRs) were supposed to be collected and analyzed at an individual level only if something suspicious was deciphered.[93] In 2002 440,606 terabytes of emails were also collected.[94] A number that is impossible to justify as warranting inspection based on probable cause. Much like the airport analogy put forth by Barry Friedman and Orin Kerr when analyzing the Fourth Amendment, people were being searched without regard to probable cause.[95] Edward Snowden's leaks about the collection of information in bulk has its supporters and critics. Regardless of public opinion of the messenger, the Second Circuit Court of Appeals ruled in May 2015 that the practices that Snowden exposed were not in fact supported

[90] Ibid.
[91] Ibid, 118-119
[92] Lyon, *Surveillance after September 11th,* 52.
[93] Franklin "Fulfilling the Promise of the USA Freedom Act."
[94] McAdams, "Internet Surveillance after September 11."
[95] See page 17.

by the Patriot Act. Despite previous presidents such as Bush and Obama referencing Section 215 as justification for the collection of American phone calls en masse, the judges reviewing the case concluded "Statues to which the government points have never been interpreted to authorize anything approaching the breadth of sweeping surveillance at issue here."[96] They also stated, many members of Congress and none of the public had an understanding of this program which lead to a lack of debate on a "momentous decision that…defies any limiting principle."[97] While it is clear liberties were taken by the state in the aftermath of September 11th it was only through a leak from a contract employee at the NSA that the information being tracked was revealed, and able to be debated. Due to this development, imperfect but substantial attempts such as the USA Freedom Act, which was passed in 2015 to limit the collection of bulk data were created.[98] This act did not do nearly as much as promised in terms of re-establishing civil liberties breached by the Patriot Act despite President Obama's reassurances. As late as June of 2018 it was reported that the NSA admitted to "technical irregularities" which lead to CDRs being collected they did not have the legal authority to obtain.[99] David Lyon and the Privacy and Civil Liberties Oversight Board argue that collecting data in this way is not an effective means to combat terrorism anyway. The Patriot Act's Section 215 and the Foreign intelligence Surveillance Act's Section 702 aimed at allowing the international communication of citizens to be monitored as "foreign intelligence" have only been associated with identifying one terrorist suspect.[100] Furthermore, David Lyon, explains in his book that the amount of information the government had was never the issue. It was the nature of their analysis. He goes as far as to say, "The most

[96]Friedersdorf, "A Federal Appeals Court Vindicates Edward Snowden's Leak of NSA Secrets."
[97] Ibid.
[98] Franklin "Fulfilling the Promise of the USA Freedom Act."
[99] Ibid.
[100] Franklin "Fulfilling the Promise of the USA Freedom Act."

vital terrorist communication may be missed (al-Qaeda groups use, but are not dependent on, the internet) the increased volume of data may simply slow the response by producing a glut. Targeted security…would deny opportunities for terrorist network activity without infringing on civil rights as present methods do."[101] Thus, this collection of data is considered overreaching by the judges on the Second Circuit Court of appeals and ineffective by scholars. Snowden also faces legal backlash should he return to the U.S. despite these developments. Effective or not, the precedent that the Patriot Act created combined with the progress that has been made in surveillance and information technology collection, means that the potential extent of what the government is surveilling is extensive. Not only does the government now have the incentive to create systems of surveillance, the actual infrastructure of the internet and therefore information technology runs on a system that can easily be commandeered by a central power.[102]

As mentioned above, the events that shook the world on September 11th have not yet been eliminated and those conducting them have begun using online tactics where attacks take place in the cyber realm. The "Information Operations Roadmap" released by the U.S. Department of Defense in 2003 shows that "U.S. and its regional allies intend on taking the war on terrorism to the internet, using a variety of means ranging from taking down 'illegal content' through to using the internet as a mean to 'deter, deny and destroy terrorist groups.'"[103] Thus, the filtering content tactics that have been used by countries like China but have not been widely utilized in democratic countries like the United States historically may be exercised under the effort to stop threats "before they are fully formed."[104] These include actions by the NSA such as their "extralegal tapping of domestic communications (including the internet) suggest, even open and

[101] Lyon, *Surveillance after September 11th*, 121.
[102] See page 12 for information on internet content filtering.
[103] Chadwick, "The Geopolitics of Internet Control Censorship, Sovereignty, and Cyberspace," 333.
[104] Ibid.

democratic societies are undertaking covert internet surveillance.[105] This can be seen in NSA's project PRISM through which the agency gained access to the systems of Google, Facebook, Apple, and other internet companies. Search history, email contents, and live chats were accessible despite the denial of knowledge of such a program by these companies' CEOs.[106] In 2018, the Department of Defense released an off-cycle report on the *Joint Concept for Operating in the Information Environment*. In it they state that "Information" is being added to the *Doctrine of the Armed Forces of the United States,* as the seventh Joint Function.[107] They also outline the ways in which they plan to apply this tool. They state, "The Joint Force applies informational power to achieve three ends: Change or maintain the observations, perceptions, attitudes, and other elements that drive desired behaviors of relevant actors. Protect and ensure the observations, perceptions, attitudes, decisions, and behaviors of the Joint Force, its allies, and its partners. Acquire, process, distribute, and employ data to enhance combat power."[108] This shows an expanded focus on this area since the release of their 2016 report in which the information environment and information power were identified.[109] With the decentralized structure of modern-day terrorist organizations and the legacy of the Patriot Act, it is unclear the limits of who will be targeted by these tactics. Especially considering the emphasis on "maintaining domestic order" in the report.[110] Thus, the parameters set out by the Patriot Act have not been effectively counteracted by the Freedom Act and are being exploited further by the state because of the changing landscape of warfare to an online platform. Thus, the technology researched as early as the 1970s regarding behavior modification is now the determined focus of the

[105] Chadwick, "The Geopolitics of Internet Control Censorship, Sovereignty, and Cyberspace," 3334.
[106] Greenwald and MacAskill. "NSA Prism Program Taps in to User Data of Apple, Google and Others."
[107] *Joint Concept for Operating in the Information Environment (JCOIE), iii.*
[108] Ibid, viii.
[109] See page 13 and 14.
[110] *Joint Concept for Operating in the Information Environment (JCOIE), vii.*

Department of Defense. The increased surveillance is also being utilized by U.S. corporations for profit. The interconnectedness of these two entities’ use of surveillance in the United States is examined in the following chapter.

Chapter 5: Corporations' and State's Aligned Interest in Information Technologies

The United States government and corporations have worked together in the past on projects like the atomic bomb and satellite technology.[111] As mentioned before the skeleton of what would become the internet (ARPAnet) was also created by the Defense Department.[112] Thus, it not surprising that the events of 9/11 were amplified by the opportunistic nature of capitalism. The desire to assert control over the internet post-9/11 means that corporations were also able to take advantage of the "new normal" that had taken hold of the information privacy infrastructure. Although 9/11 was not the beginning of corporations and governments working together, it was the catalyst for citizen acceptance. The state sold users on the idea that privacy may not be necessary in a world where their protection depended on it being invaded and they would be taught to enjoy the convenience of corporation's predictive controls.

The CIA and the NSA knew in the 1990s that intelligence and supercomputing may mean that their work may be moving outside the sphere of the government system. This was compounded by the lack of funding they were receiving, and the immense wealth Silicon Valley was accumulating at the time. Thus, the private sector and the intelligence community came together to create The Massive Digital Data Systems Project (MDDS). Computer scientists at leading universities such as Stanford, MIT, Caltech, and Harvard were recruited and given a white paper brief that told them what these institutions were looking to achieve and could later be expanded by the private sector if their projects were successful. In the 1993 MDDS white paper it stated that the Intelligence Community (IC) is "taking a proactive role in stimulating research in the efficient management of massive databases and ensuring that IC requirements can

[111] Nesbit, "Google's True Origin Partly Lies In CIA And NSA Research Grants For Mass Surveillance."
[112] See page 21.

be incorporated or adapted into commercial products."[113] Millions of dollars were directed through the National Science Foundation so that the most successful projects could be used to create the type of companies attracting investment in Silicon Valley. Some successful companies that were created through this program include, Qualcomm, Symantec, and Netscape. Other projects researched areas like fiber optics which are essential to AccuWeather, Verizon, and the major internet provider for a large part of the U.S. like AT&T. The National Science Foundation (NSF), as of 2017 still provides 90% of federal funding to universities for computer-based research. One such project labelled "birds of a feather" was aimed at sorting digital information on users such as their online queries in order of importance, type etc. Thus, allowing specific communities to be tracked by their common interests. Essentially tracking groups digital fingerprints. The goal was to be able to identify terrorists and criminals. Two such grants funded by the NSA and CIA were given to Larry Page and Sergey Brin, Google's co-founders. One grant funded by NSF and the Defense Advanced Research Projects Agency (DARPA) was given to them with the goal of creating a "digital library," which would turn the information on the internet into easily searchable material. The other grant had the objective of "query optimization of very complex queries that are described using the 'query flocks' approach."[114] In other words, implementing the "birds of a feather" project. While the "digital libraries" grant is mentioned in Google's origin story, the MDDS intelligence community grant is not.[115] Google has denied entanglement with the CIA as well. However, there are recent projects that make Hamlet's quote "thou dost protest too much" come to mind after reviewing Google's connection to government programs both in the U.S. and in China.

[113] Nesbit, "True Origin Partly Lies in CIA and NSA Research Grants For Mass Surveillance."
[114] Ibid.
[115] Ibid.

Google's CEO Eric Schmidt in 2009 said, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[116] This sentiment combined with projects such as, Dragonfly and Maven have left many Google employee's feeling the removal of the statement, "Do no evil" from the preamble of their code of conduct. Before the revision, this phrase appeared multiple times throughout the document. Now it is only mentioned once in the 6,313-word piece in the sentence encouraging employees to speak up if they see something they don't feel is right.[117] Despite appointing Ross LaJeunesse to specifically protect human rights in China after announcing in January of 2010 that Gmail accounts of Chinese Human Rights Activists had been breached which prompted them to stop censoring searches in China (which they had been doing since January 2006 when Google.cn was founded). Google secretly reengaged in catering the Chinese authoritarian regime by secretly taking on a project named Dragonfly in 2017.[118] In protest 1,400 employees signed an internal letter in response to the lack of transparency in regard to plans to work with China.[119] While they ended the project in 2019, they have not committed to ensuring such a search engine is not created by them again for the Chinese market.[120] Furthermore, Google created an AI Center in Beijing in December 2017 despite LaJenesse's protests reminding Google that business in China is inextricably linked with the government. During this same period Google cloud-computing section was working on Project Maven. The goal of the project for the Pentagon was to provide computer vision technology for drones.[121] Despite Google's encouragement to employees to say something if they felt their ethics were not in the right place, some dozen resigned after 3,100 of Google's

[116] Lee, *Facebook Nation: Total Information Awareness*, 401.
[117] Cuthbertson, "Google Just Quietly Removed References To 'Don't Be Evil' From Its Code of Conduct."
[118] Su, "Confirmed: Google Terminated Project Dragonfly, Its Censored Chinese Search Engine."
[119] Ibid.
[120] Su, "Confirmed: Google Terminated Project Dragonfly, Its Censored Chinese Search Engine."
[121] Ibid.

employees signed an open letter asking the company to stop the project in 2018.[122] Many feared Google's users' personal data would be combined with the military surveillance to help achieve targeted killings.[123] While Google did decide not to renew the contract because of the dissent it received, it did not do so before many lost their jobs. There is also nothing preventing another company from taking the place of Google and using the data they have collected on users in the same way. Ross LaJeunesse lost his position in April of this year. He told the *Washington Post* this was due to his constant pushing of a human rights program meant to formalize Google's support of free expression and privacy. According to one of Google's lawyers and head of policy this suggestion was denied because it could increase Google's liability. Jenn Kaiser, Google's spokeswoman said LaJuenesse was removed from the company because of a "reorganization of our policy team."[124]

Google is not the only company working closely with the United States and Chinese governments. China's big data industry has been growing exponentially in the last 6 years. It grew from an 8.4-billion-yuan market in 2014 to 57.8 billion-yuan in 2020.[125] It is also the world's most populous country. Therefore, it is a prime market for upcoming and established technology companies. Microsoft has been in China since 1992. The company helped create the government's computer systems, including a version of Windows that complies with China's censorship controls. Along with Google, Cisco, and Yahoo, Microsoft also helped build the Great Firewall of China.[126] Government contracts can bring in substantial sums of money for these companies. This is why Microsoft and Amazon fought just this year for the Pentagon's

[122] Cuthbertson, "Google Just Quietly Removed References To 'Don't Be Evil' From Its Code of Conduct."
[123] Ibid
[124] Su, "Confirmed: Google Terminated Project Dragonfly, Its Censored Chinese Search Engine."
[125] Wong, "China: Big Data Market Size 2014-2020."
[126] Bass, and Banjo. "Microsoft's Long History in China Complicates Potential TikTok Deal."

Joint Enterprise Defense Infrastructure (JEDI) project worth 10 billion dollars. Microsoft was awarded the project and is now tasked with designing cloud services such as artificial intelligence processing, machine learning, storage, and the ability to process “mission critical workloads.”[127] How these systems will be created and whether they will use user data is not clear at this point. Microsoft is also working with the government to produce the Integrated Visual Augmentation System (IVAS) HoloLens. An augmented reality headset for combat that will track soldier’s data such as their location and heart rate to increase efficiency. A base in Austin, Texas, named the Futures Command base, is set up to allow small and large tech companies alike to bring their technology to the battlefield.[128]

[127] Lyons, “The Pentagon Says Microsoft Should Still Get Its $10B JEDI Contract Following an Investigation.”
[128] Haselton, “How the Army Plans to Use Microsoft's High-Tech HoloLens Goggles on the Battlefield.”

Chapter 6: Misuse of User Data and its Consequences

The above actions of technology corporations illustrate the power of the companies domestically and globally as well as the relationship they have with various governments. As can be seen, user information is a tool that powers innovation and contracts. As mentioned before, user agreements are often long, blanketed statements that must be accepted before access is given to technology. However, these contracts are only between the user and the company and can be changed at the discretion of the company. If the user does not wish to stop using the products, they have to accept the new policies. Unsurprisingly, "it has been observed that data subject [users] often do not read complex data protection policies, and in any case, given the fact that access to services and goods on the market of the information society relies on a few number of monopolistic providers, data subject would not have a real free choice."[129] Google replaced over 60 different privacy policies across Google products in March of 2012.[130] In the announcement of this new policy, they admitted to data mining user information across platforms. Whether the user is on YouTube, an Android phone or Gmail, what is being searched, or discussed on the platforms is now used to "tailor your search results."[131] While this may be convenient for some, "search data can reveal particularly sensitive information about you, including facts about your location, interests, age, sexual orientation, religion, health concerns, and more."[132] These new policies do not allow users to opt out either. They must be accepted and if the user has enough technological literacy to know where to look, they may go to their settings and filter through the pages of information the company automatically collects and change the settings. On Google's Privacy Policy page, it states, "The information we collect includes unique

[129] Contissa, *Information technology for the Law,* 115.
[130] Lee, Newton, *Facebook Nation: Total Information Awareness*, 50.
[131] Ibid.
[132] Ibid.

identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP addresses, crash reports, system activity, and the date, time, and referrer URL of your request." Furthermore, it states under the "Your Activity" section, that the videos, purchases, terms searched, people you share information with, and activity on third-party sites and apps that use their services are also monitored and stored. This takes place even when users are not logged in to a Google account. The "unique identifiers tied to the browser, application, or device you're using…help us to do things like maintain your language preferences across browsing sessions." Should you sign they will use this information as "personal information" tied to the Google Account. Google states they do not share this information unless it needs to for external processing "to our affiliates" or for legal reasons. However, Google's list of affiliate companies is growing daily. Not to mention when signing in to almost any site, you can choose to use your Google account, therefore, linking activity after activity to your "unique identifiers."[133] Much of this information is used to create micro-targeted advertising. This information is used to create a profile on users allowing companies like Google to sell its ability to create unique identifiers to companies as part of their advertising package. This ensures the products that are advertised to consumers are more likely to fit their personality and lifestyle. It is also the type of information that Cambridge Analytica used in the Brexit campaign in England and in the 2016 presidential election to gain votes from undecided voters.

While this thesis will not go into detail about any particular campaign, how data is being used in the digital world in political campaigns needs to be briefly mentioned. There are now

[133] Google. "Privacy Policy – Privacy & Terms," September 30, 2020.

over 250 companies that specialize in using individual's data for political campaigns. Some of these companies are, Cambridge Analytica, BlueStateDigital, and eXplain.[134] Their value lies in the company's ability to gather specific information on people through their online activity to achieve personalize targeted communication. According to the International Institute for Democracy and Electoral Assistance (IDEA), political campaigns "'increasingly use big data on voters and aggregate them into datasets' which allow them to 'achieve a highly detailed understanding of the behaviour, opinions and feelings of voters, allowing parties to cluster voters in complex groups'"[135] This also allows for "look-alike audiences" to be found. In other words, groups that are similar to those already pledged to a campaign in behaviors or interests, but who have not yet decided how they will vote. According to the UK Information Commissioner, Elizabeth Denham, "fair practices and fair democracy is under threat if large data companies are processing data in ways that are invisible to the public."[136] The U.S. Senate Select Committee on Intelligence, and the European commission of shared similar concerns regarding the use of this information by political campaigns.[137]

This type of data is gathered by many different companies. Microsoft partnered with its search engine Bing, Twitter and Facebook to collect similar information as well as share with your friends what it is you are browsing.[138] If you agree with Eric Schmidt and feel if you are doing something that you don't want people to know perhaps you should not be doing it, you may not take issue with these standards. However, what if you are a homosexual, have a criminal record, or just don't want your grandparents to know what you are searching for? As a user can

[134] Dommett, "Data-Driven Political Campaigns in Practice: Understanding and Regulating Diverse Data-Driven Campaigns," 7.
[135] Ibid, 8.
[136] Ibid.
[137] Ibid, 6.
[138] Lee, *Facebook Nation: Total Information Awareness*, 50.

you be certain the information gathered by these companies won't suddenly become available to those searching your profile or linked to your account in some way? This exact event occurred in 2011 when Bing was integrated with Facebook. "''Friends' pictures, cities of residence, education, employment details, travel locations, and even shopping lists" became available through the social search.[139] Thus, the "Friend Effect" was created. Users could make decisions on topics they searched with the approval of friends without ever speaking to them simply by viewing their online activity. User data can also come into play when they are hired or applying for loans depending on the software that scans your resume or that the bank runs your profile through. According to Giuseppe Contissa in *Information Technology for the Law*, "an algorithm processes a slew of statistics and comes up with a probability that a certain person might be a bad hire, a risky borrower, a terrorist, or a miserable teacher. The probability is distilled into a score, which can turn someone's life upside down. And yet when the person fights back 'suggestive' countervailing evidence simply won't cut it. The case must be ironclad. The human victims…are held to a far higher standard of evidence than the algorithms themselves."[140] While Google or Microsoft user profiles are not yet integrated with these systems, companies frequently view potential hires' social media presence and if your profile is private, employers may wonder what you have to hide. Thus, these systems begin to resemble the "Social Credit System" in China with those who play along getting rewarded and those that do not get punished.

As the ability to create files on users expands to the internet of things, other aspects of life can be controlled. Applications such as Foursquare and the "Find my Friend" Application on Facebook (applications labeled ambient applications because they use the GPS on a device) were

[139] Ibid.

[140] Contissa, *Information technology for the Law,* 109-110.

created to help friends connect while also allowing companies to advertise restaurants and businesses to users based on their location. However, this technology also led to the creation of "Girls Around Me" in 2012. This application showed users pictures of girls in the neighborhood who were nearby. As the potential implications could have been disastrous it was removed. But not before it was downloaded 70,000 times. Facebook still has a Find My Friend application that users now need to opt into.[141] Another example is the "vehicular monitoring systems." By using real-time GPS information and user data car and insurance companies could stop the car from turning on if payments are not made or change customers insurance plans based on their driving habits.[142] Furthermore, when agreeing to privacy policies the user is assuming the company will protect their information or at least limit its use to the company's internal projects. Therefore, should the company have a data breach, it is up to the company to determine what information has been accessed and how to rectify the situation. Users may never discover that their information has been used in a way they did not agree to at all.

One prominent example of this blatant misuse of user information can be seen in the collection and utilization by Clearview AI. A company that was able to invent and distribute their services, without any input from the public or legislators. The company's operations were revealed by the *New York Times* in 2016. It was released that they had scraped Facebook, Venmo, Twitter, LinkedIn, Instagram, and other such sites for photos despite the user agreements on each of these sites. The tool they created was a search engine much like Google or Bing. But instead of information as a subject, you could upload a photo and be given the digital history of the person whose face was analyzed by the system. This information was then turned

[141] Lee, *Facebook Nation: Total Information Awareness*, 43.
[142] Zuboff, *Surveillance Capitalism*, 215.

into a surveillance tool that was sold to local police. When the *New York Times* article was published, it was estimated 600 law enforcement agencies had started using the product. This technology has allowed for some cases to be solved in record time but has also led to the incorrect detainment of those misidentified by the system This tool was developed by the company and sold directly to the police.[143] This means the information collected on users was utilized by both the company and by the police through the system without any input from civil society or government organizations. It was only after the *New York Times* article that the companies whose systems were scraped were aware of the breach. Even then, the cases filed by these companies were on behalf of themselves and the misuse of their data. A lawsuit filed on behalf of the consequences this could have on citizens was filed by the ACLU in May of this year. According to this lawsuit, Clearview AI's actions not only were a breach of privacy policies but of the Biometric Information Privacy Act (BIPA) in Illinois, one of the state's this software is being used in.[144] The ACLU claims this this software can have a detrimental impact on Latinas and survivors of abuse. Linda Tortolero, the CEO of Mujeres Latinas en Acción stated, "this technology isn't just unnerving, it's dangerous, even life-threatening. It give free rein to stalkers and abusive ex-partners, predatory companies, and ICE agents to track and target us."[145] Mallory Littlejohn from the Chicago Alliance Against Sexual Exploitation said, "We can change our names and addresses to shield our whereabouts and identities from stalkers and abusive partners, but we can't change our faces."[146] This software caught the ACLU's attention in Michigan as well. Robin Julian-Borchak Williams was detained for 30 hours by Detroit police for a theft he did not commit based on the facial recognition software. His case was dismissed

[143] Hill, "The Secretive Company That Might End Privacy as We Know It."
[144] ACLU. "ACLU Sues Clearview AI."
[145] Ibid.
[146] ACLU. "ACLU Sues Clearview AI."

but “without prejudice.” This means he can be tried again; despite the fact it was proven he was not the man in the video despite the software’s declaration.[147] This reliance on software shows the cultural “assumption of fairness or objectivity” when decisions are made by computer algorithms. It occurs so often; it has a dedicated term to describe the phenomena. “Data fundamentalism, namely the tendency to believe that the correlation assessed by the algorithm implies causality, and that the analysis carried out with data mining techniques on large sets of data always provides an objective view of reality.”[148] This occurs despite the fact that these “systems can be vulnerable to a variety of problems that can result in systematically faulty and biased determinations.”[149] This is because humans are flawed and have built in biases and they responsible for the creation of these systems. The National Institute of Standards and Technology in a study produced in December 2019 showed that “incorrect associations of two subjects” by facial recognition systems were “2 and 5 times higher in women than men.” They also found false positives or incorrect associations of one face with another were the worst in African Americans and Asian populations.[150] These statistics apply to government databases like the FBI’s Next Generation Identification System that use facial recognition algorithms based on their mugshots database.[151] However, the case of Robin Williams in Michigan shows that even though Clearview AI’s system has a more extensive database, the algorithms can still be programed with flaws and biases. The affiliates of the ACLU have shown clear alarm at the creation of this software because of the potential use by government agencies. This alarm is clearly not

[147] Hill, “Wrongfully Accused by an Algorithm.”
[148] Contissa, *Information Technology for The Law*, 111.
[149] Ibid.
[150] Grother, “Face recognition vendor test part 3,” 2-8.
[151] Deneyer, “China's Watchful Eye.”

misplaced. Local police, the FBI, and ICE are now all using similar tools to gather information on people, track dissent, as well as solve crimes.

Commercial data brokers serve as the middlemen between law enforcement and commercial data. While due process still applies to obtaining warrants in someone's home, their personal information that is available online can be purchased without one.[152] According the United States Marshals Service, "With as little as a first name or a partial address, you can obtain a comprehensive personal profile in minutes. The profile includes personal identifying information (name, alias name, date of birth, social security number), all known addresses, drivers license information, vehicle information... telephone numbers, corporations, business affiliations, aircraft, boats, assets, professional licenses, concealed weapons permits, liens, judgments, lawsuits, marriages, worker compensation claims, etc."[153] According to an article in the Public Contract Law Journal published in 2009, "Some brokers also "maintain unlisted phone numbers and details about people's occupations, religions, and ethnicities. They sometimes know what some people read, what they order over the phone and online, and where they go on vacation."[154] According to the 2013 report by the World Privacy Forum, law enforcement spends billions of dollars on this type of information.[155] Companies that provide this type of information include Acxiom, Experian, LexisNexis, and ChoicePoint, now a LexisNexis company.[156]

The Black Lives Matter movement exploded across the U.S. this summer after a video of George Floyd was shown in which he states he cannot breathe several times while an officer

[152] Hoofnagle, ""Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement," 595.
[153] Ibid. 596
[154] McCain, "Applying The Privacy Act Of 1974 To Data Brokers Contracting With The Government," 936.
[155] Gelleman and Dixon, *Data Brokers and the Federal Government: A New Front in the Battle for Privacy Opens*, 8.
[156] McCain, "Applying The Privacy Act Of 1974 To Data Brokers Contracting With The Government," 935.

kneels on his neck. After his death, the movement gained significant traction. Images of protesters could be seen across news outlets and social media platforms. The FBI and local police used this exposure to identify protest organizers and participants. In Cookeville, Tennessee those involved were targeted at home and at work and were brought in for questioning. The Department of Homeland Security has been monitoring the spread of this movement through social media since 2015. Immigration and Customs Enforcement has also used Facebook to track protests against immigration and gun-control policies. These were used to create a list of activists, journalists, Facebook group administrators, and lawyers that were then classified as deserving "greater scrutiny" at the US-Mexico border.[157] The government also has automated license plate readers, Stingray devices (which allow police to track cell phones and discover phone numbers of those in the vicinity), facial recognition, and drones with cameras.[158] They are not being used just to target protesters either. Police have been using algorithms to predict where crimes are likely to occur.[159] These tools and applications alone mirror those used in China. However, the targeting by authorities of those exercising their right peacefully to protest is the proverbial straw that may break the back of our democracy.

[157] Funk, "How Domestic Spying Tools Undermine Racial Justice Protests."
[158] Ibid.
[159] Deneyer, "China's Watchful Eye."

Conclusion: China and the United States - Concurrent or Contrasting Realities?

Minorities being further disenfranchised, authorities monitoring civilians, companies profiting from government contracts, and micro-targeting based on user profiles are all common traits between the United States and China's use of surveillance technology. Both the United States and China are exporting their technologies, and both are continuing to innovate products that incorporate data mining through big data found on the ubiquitous internet of things. United States and Chinese companies work with their governments and the others to access both. Is the result a trend toward authoritarian tendencies in the United States? This study makes a case for this argument in the affirmative.

The hypothesis at the beginning of this thesis stated: *While the type of political rule created vastly different types of information technology when the internet was first created, the pressure international terrorism put on state security concerns, and the use of surveillance capitalism by corporations have been compounded by the lack of transparency in their use. The result is that the gap between information technology in authoritarian and democratic governments has diminished over time.* It was also stated that the limits on the collection of personal data, rights for individuals subject to data collection, the ability to hold entities accountable, and the transparency in the process would be taken into consideration. These parameters were to be combined with the metrics on page sixteen to determine whether the United States' democracy was being negatively influenced by these technologies. The questions raised about the application of this technology in relation to the fourth amendment were answered in the cases showing the targeting of protesters in both countries. Limiting their ability to exercise their right to free speech and peaceful assembly go against the democratic norms referenced in these metrics. The lack of alternative choices to privacy policies and to how data is used by companies when it is collected goes against the second metric. The creation of Clearview AI without public or government input, the use of commercial data brokers by law-enforcement without user consent, and the possible use of user data to develop government projects like Google's Maven for the Pentagon or Microsoft's JEDI, are just a few illustrations of a lack of transparency in the process. Violence both direct and indirect can be seen because of these technologies. Only a few examples were given such as the risk to women through the "Girls Around Me" application, Latinas, survivors of sexual abuse, and those targeted by authorities in the U.S. and China such as, the Uyghurs, and the Hong Kong and Black Lives Matter protestors. Other examples were given of technology created for one purpose, such as targeted advertising and used in another like influencing election results. All of this clearly shows the "willingness to curtail the civil liberties of opponents" and the citizenry as a whole. This does not however, mean that the United States must continue on this path.

The United States is still for all intents and purposes a democracy backed by the rule of law. The "rule of truth" has not yet been widely applied as it has in China. However, the book *Information Technology for the Law* that was published in 2017 states, "the law is just starting to look at the issues raised by the combination of data mining techniques and algorithmic decision-making process."[160] Companies and the United States government have been creating such systems since the 1970s, therefore, one must wonder how much longer the law will take to catch up with these programs or if it ever will.[161] Europe's GDPR, California's Consumer Privacy Act and Illinois' Biometric Information Privacy Act are all steps in the right direction. Yet, the same year the Consumer Privacy Act was passed, Proposition 25 was proposed in California. This

[160] Contissa, *Information Technology for The Law*, 109.
[161] See page 39.

proposition would have replaced cash bail with an algorithm that would determine whether the accused should be released before trial. This also came after SB 10 was passed in conjunction with SB 36 in 2018 and 2017, respectively. These were aimed at creating a system to mitigate the bias of algorithmic systems after a report from the American Psychological Association showed throughout the country nine out of ten pretrial detention agencies use such a system along with 28 states using them for parole decisions and 20 states for sentencing.[162] While these made external audits a means to combat this bias, who is determining what is bias and fair is not clear, nor was it further outlined in Proposition 25. Furthermore, these mitigation efforts were only made clear to those who looked into the program as no information was provided to voters on the subject. No information on who would produce the algorithmic system could be identified either. This example shows that even when legislation is applied to this technology the process is slow and littered with issues. With regard to the GDPR legislation, consent and purposes of data use, the use of pseudonymization of data, and transparency are all topics outlined by the legislation. However, it has already been determined the legislation focused on these areas have significant flaws. The uses of data in ways that prove valuable is not usually known when the data is collected. Yet this is when the GDPR determined purposes of data collection should be made known. It has also been shown "that the adoption of technical measures for pseudonymisaiton [sic] may not provide…privacy nor fairness."[163] Lastly, imperative terms such as transparency lack an agreed upon definition.[164] Thus, it would seem the rule of law is not current enough or comprehensive enough to truly protect citizens from the authoritarian tendencies of information technology as it is currently structured. Furthermore, as has been

[162] Johnson, "California's Prop 25 Would Replace Cash Bail with Algorithms, but Questions around Fairness and Transparency Remain."
[163] Contissa, *Information Technology for The Law* 115.
[164] Ibid. 115-116

shown, data is an economic driver. Consequently, politicians wishing to get elected may not wish to unsettle a thriving economy as it could hurt their chances of re-election. Corporations are also relentless about lobbying to ensure their main source of income online is protected. It is therefore, up to the people to ensure these concerns are a focus of future legislators.

The purpose of this thesis was to appropriately alarm the masses by showing the similarities of China and the United States with regard to information technology. There are many more instances of misuse of data, cooperation of U.S. companies with China and the U.S. government whilst using user data in ways they are unaware of. So many, books and sections of libraries have been dedicated to them. Corporations and states have been made aware of the many forms of information power and surveillance capitalism, but the masses are still largely in the dark. It is the duty of the state, legislators, civil society, journalists, and organizations to ensure the use of information technology does not continue down a path that will lead to an authoritarian use-case. It is hoped this thesis will be part of a larger effort to continue to research, report, and change the use of information technology until systems are put in place that truly protect users from unwarranted surveillance. Commissions should be created at the state and local level with experts from various fields such as lawyers, engineers, and civil rights organizations to create legislation that allows users to opt-in to these pervasive information systems instead of opt-out. Efforts should be made to build on existing legislation to ensure this technology is used in a way that aligns with the democratic values the United States and the internet were founded on. The fact that this technology has permeated almost every aspect of society means that this shift will not take place overnight. Instead the efforts will be akin to the turning of a large boat. In the United States, it is up to the people, not one authority, to determine the direction of society. Therefore, provided those at the helm in the United States make the effort, the ship should eventually arrive at a more democratic destination.

Bibliography

ACLU. "ACLU Sues Clearview AI." American Civil Liberties Union, May 28, 2020. https://www.aclu.org/press-releases/aclu-sues-clearview-ai.

Andrew, Philip N. Howard, and Ronald J Deibert. "The Geopolitics of Internet Control Censorship, Sovereignty, and Cyberspace." In *Routledge Handbook of Internet Politics*, 323–36. London: Routledge, 2010.

Bass, Dina, and Shelly Banjo. "Microsoft's Long History in China Complicates Potential TikTok Deal." Bloomberg.com. Bloomberg, August 3, 2020. https://www.bloomberg.com/news/articles/2020-08-03/microsoft-s-long-history-in-china-complicates-potential-tiktok-deal.

Brandom, Russell. "We Have Abandoned Every Principle of the Free and Open Internet," December 19, 2017. https://www.theverge.com/2017/12/19/16792306/fcc-net-neutrality-open-internet-history-free-speech-anonymity.

Brewster, Thomas. "Border Patrol Spent $2 Million On Google Maps For A Massive Surveillance Tool." Forbes. Forbes Magazine, October 15, 2020. https://www.forbes.com/sites/thomasbrewster/2020/10/13/cbp-spent-2-million-on-google-maps-for-a-massive-surveillance-tool/.

Broussard, Meredith. Artificial Unintelligence: How Computers Misunderstand the World. Cambridge: MIT Press, 2018. Accessed November 19, 2020. ProQuest Ebook Central.

Caffrey, Cait. "2019 Hong Kong Anti-Extradition Bill Protests." *Salem Press Encyclopedia*, 2019.http://search.ebscohost.com.proxy.library.nyu.edu/login.aspx?direct=true&db=ers&AN=\140435609&site=eds-live.

Canadian Security Intelligence. "Government of Canada," May 17, 2018. https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html.

Castells, Manuel. The Rise of the Network Society : The Information Age - Economy, Society and Culture. Hoboken: John Wiley & Sons, Incorporated, 2009. Accessed November 19, 2020. ProQuest Ebook Central.Chadwick,

Chan, Edwin. "The Great Firewall of China." Bloomberg.com. Bloomberg, 2015. https://www.bloomberg.com/quicktake/great-firewall-of-china.

Chan, Tara Francis. "16 Parts of China Are Now Using Skynet, the Facial Recognition Tech That Can Scan the Country's Entire Population in a Second," March 27, 2018.

https://www.businessinsider.com.au/china-facial-recognition-technology-works-in-one-second-2018-3.

Chen, Angela. “IBM's Watson Gave Unsafe Recommendations for Treating Cancer,” July 26, 2018. https://www.theverge.com/2018/7/26/17619382/ibms-watson-cancer-ai-healthcare-science.

Chen, Yu-Jie, Ching-Fu Lin, and Han-Wei Liu. “Rule of Trust: The Power and Perils of China’s Social Credit Megaproject.” *Columbia Journal of Asian Law* 32, no. 1 (2018): 1–36. http://search.ebscohost.com.proxy.library.nyu.edu/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.colas32.4&site=eds-live.

Chin, Josh, Clément Bürge, and Giulia Marchi. “Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life,” December 20, 2017. https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355.

Cohen, J. E. (2019). *Between truth and power : The legal constructions of informational capitalism*. ProQuest Ebook Central https://ebookcentral-proquest-com.proxy.library.nyu.edu

Contissa, Giuseppe. Information technology for the law. Turin: G. Giappichelli, 2017. Accessed November 20, 2020. ProQuest Ebook Central.

Dommett, Katharine. “Data-Driven Political Campaigns in Practice: Understanding and Regulating Diverse Data-Driven Campaigns.” Internet Policy Review ume 8, no. Issue 4 (December 1, 2019). doi:10.14763/2019.4.1432.

Deneyer, Simon. “China's Watchful Eye,” January 7, 2018. https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/.

Department of Defense. (2018). *Joint Concept for Operating in the Information Environment (JCOIE)* (Rep.). Washington, D.C: Department of Defense.

Department of Defense. (2016). *Strategy For Operations In The Information Environment* (pp. 2-15, Rep.). Washington, D.C: Department of Defense. doi:https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

Dyann Heward-Mills; Helga Turku, "California and the European Union Take the Lead in Data Protection," Hastings International and Comparative Law Review 43, no. 2 (Summer 2020): 319-338

Franklin, Sharon B. “Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records.” Just Security, March 28, 2019.

https://www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records/.

Freedom House. “Press Release: Freedom on the Net 2019 Reveals Crisis on Popular Platforms.” Freedom House, 2019. https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/press-release.

Freidman, Barry, and Orin Kerr. “The Fourth Amendment.” Interpretation: The Fourth Amendment | The National Constitution Center. Accessed November 19, 2020. https://constitutioncenter.org/interactive-constitution/interpretation/amendment-iv/interps/121.

Friedersdorf, Conor. “A Federal Appeals Court Vindicates Edward Snowden's Leak of NSA Secrets.” The Atlantic. Atlantic Media Company, May 11, 2015. https://www.theatlantic.com/politics/archive/2015/05/the-vindication-of-edward-snowden/392741/.

Funk, Allie. “How Domestic Spying Tools Undermine Racial Justice Protests.” Freedom House, June 22, 2020. https://freedomhouse.org/article/how-domestic-spying-tools-undermine-racial-justice-protests.

Galloway, Alexander R.. Protocol : How Control Exists after Decentralization. Cambridge: MIT Press, 2004. Accessed November 19, 2020. ProQuest Ebook Central.

Gelleman, Robert and Dixon Pam. Rep. Data Brokers and the Federal Government: A New Front in the Battle for Privacy Opens. Vol. 3. Lake Oswego, OR: World Privacy Forum, 2013. Global Times. “Surveillance Tech Grows in Xinjiang, Necessary to Counter Terrorism.” Global Times, 2018. https://www.globaltimes.cn/content/1109176.shtml.

Greenwald , Glenn, and Ewen MacAskill. “NSA Prism Program Taps in to User Data of Apple, Google and Others.” The Guardian. Guardian News and Media, June 7, 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Grother , Patrick, Mei Ngan, and Kayee Hanaoka. Rep. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. Department of Commerce, 2019.

Google Official Blog. (2010, January 12). A new approach to China. Retrieved October 28,

2020, from https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

Google. “Privacy Policy – Privacy & Terms,” September 30, 2020. https://policies.google.com/privacy?hl=en-US.

Gueorguiev, Dimitar. “Analysis | Mike Bloomberg Said China Isn't a Dictatorship. Is He Right?” The Washington Post. WP Company, December 4, 2019.

https://www.washingtonpost.com/politics/2019/12/04/michael-bloomberg-said-china-isnt-dictatorship-is-he-right/.

Heward-Mills, Dyann, and Helga Turku. “California and the European Union Take the Lead in Data Protection.” *Hastings International and Comparative Law Review* 43, no. 2 (2020): 319–38.

Hill, Kashmir. “The Secretive Company That Might End Privacy as We Know It.” The New York Times. The New York Times, January 18, 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Hill, Kashmir. “Wrongfully Accused by an Algorithm.” The New York Times. The New York Times, June 24, 2020. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

Hillman, Jonathan E., and Maesea McCaplin. “Watching Huawei's ‘Safe Cities.’” Watching Huawei's "Safe Cities" | Center for Strategic and International Studies, November 15, 2020. https://www.csis.org/analysis/watching-huaweis-safe-cities.

Hoofnagle, Chris Jay. “Big Brother’s Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement.” *North Carolina Journal of International Law and Commercial Regulation* 29, no. 4 (2003): 595–638. http://search.ebscohost.com.proxy.library.nyu.edu/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.ncjint29.26&site=eds-live.

H.R. Rep. No. Hearing Before The Subcommittee On Asia, The Pacific And Nonproliferation Of The Committee On Foreign Affairs House Of Representatives One Hundred Sixteenth Congress-Authoritarianism With Chinese Characteristics: Political And Religious Human Rights Challenges In China (2019).

Human Rights Watch. (2020, October 28). China: Police 'Big Data' Systems Violate Privacy, Target Dissent. Retrieved November 07, 2020, from https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent

Huawei Investment & Holding Co. Ltd. 2019 Annual Report.

Jeffries, Stuart. “How the Web Lost Its Way – and Its Founding Principles.” The Guardian. Guardian News and Media, August 24, 2014. https://www.theguardian.com/technology/2014/aug/24/internet-lost-its-way-tim-berners-lee-world-wide-web.

Jie, Shan. “China Exports Facial ID Technology to Zimbabwe,” 2018. https://www.globaltimes.cn/content/1097747.shtml.

Johnson, Khari. “California's Prop 25 Would Replace Cash Bail with Algorithms, but Questions around Fairness and Transparency Remain.” VentureBeat. VentureBeat, November 3, 2020. https://venturebeat.com/2020/11/03/the-unavoidable-glaring-cproblem-with-californias-prop-25-to-replace-cash-bail-with-an-algorithm/.

Joppke, Christian. "Why Liberal States Accept Unwanted Immigration." *World Politics* 50, no. 2 (1998): 266-93. Accessed November 19, 2020. http://www.jstor.org/stable/25054038.

Lee, Newton. Facebook Nation: Total Information Awareness. New York, NY: Springer New York, 2014. Accessed November 15, 2020. ProQuest Ebook Central.

Levitsky, Steven, and Daniel Ziblatt. *How Democracies Die*. New York, NY: Broadway Books., 2019.

Lewis, James. “Cognitive Effect and State Conflict in Cyberspace.” Cognitive Effect and State Conflict in Cyberspace | Center for Strategic and International Studies, November 16, 2020. https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace.

Linz, Juan. *The breakdown of democratic regimes: crisis, breakdown, and reequilibration.* Baltimore: Johns Hopkins University Press. 1978

Lyons, Kim. “The Pentagon Says Microsoft Should Still Get Its $10B JEDI Contract Following an Investigation.” The Verge. The Verge, September 4, 2020. https://www.theverge.com/2020/9/4/21423312/pentagon-microsoft-jedi-amazon-trump-defense-contract-cloud-bezos.

Mahtani, Shibani. “Masks, Cash and Apps: How Hong Kong's Protesters Find Ways to Outwit the Surveillance State .” The Washington Post. WP Company, June 15, 2019. https://www.washingtonpost.com/world/asia_pacific/masks-cash-and-apps-how-hong-kongs-protesters-find-ways-to-outwit-the-surveillance-state/2019/06/15/8229169c-8ea0-11e9-b6f4-033356502dce_story.html.

McAdams, James. "Internet Surveillance after September 11: Is the United States Becoming Great Britain?" *Comparative Politics* 37, no. 4 (2005): 479-98. Accessed November 19, 2020. doi:10.2307/20072905.

McCain, James. "Applying The Privacy Act Of 1974 To Data Brokers Contracting With The Government." Public Contract Law Journal 38, no. 4 (2009): 935-53. Accessed December 9, 2020. http://www.jstor.org.proxy.library.nyu.edu/stable/25755743.

Mozur, Paul. “Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras.” The New York Times. The New York Times, July 8, 2018. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

Open Net Initiative. (2012, August). China. Retrieved October 17, 2020, from https://opennet.net/research/profiles/china-including-hong-kong

Ovide, Shira. “The Real Dangers of Surveillance.” The New York Times. The New York Times, June 12, 2020. https://www.nytimes.com/2020/06/12/technology/surveillance-protests-hong-kong.html.

Senate No. Subcommittee on Technology, Terrorism, And Government Information Of The Committee On The Judiciary United States Senate One Hundred Seventh Congress Second Session (2002).

The World Wide Web Foundation. (n.d.). History of the Web. Retrieved September 19, 2020, from https://webfoundation.org/about/vision/history-of-the-web/?gclid=EAIaIQobChMI1LeZqfn16wIVCtvACh0HOgfEEAAYASAAEgKPtfD_BwE

Ünver, H. Akın. Report. Centre for Economics and Foreign Policy Studies, 2018. Accessed November 19, 2020. http://www.jstor.org/stable/resrep17009.

Wahman, Michael, Jan Teorell, and Axel Hadenius. “Authoritarian Regime Types Revisited: Updated Data in Comparative Perspective.” *Contemporary Politics* 19, no. 1 (January 1, 2013): 19–34. doi:10.1080/13569775.2013.773200.

Wong, Samantha. “China: Big Data Market Size 2014-2020.” Statista, December 20, 2019. https://www.statista.com/statistics/796500/china-big-data-market-size/.

Qiang, Xiao. “The Road to Digital Unfreedom: President Xi’s Surveillance State.” *Journal of Democracy* 30, no. 1 (2019): 53–67.

Shipler, David K. “It's Time for a 21st Century Debate on Privacy and Surveillance.” The Nation, June 29, 2015. https://www.thenation.com/article/archive/its-time-21st-century-debate-privacy-and-surveillance/.

Xinhuanet. “China Signs 197 B&R Cooperation Documents with 137 Countries, 30 Int'l Organizations,” 2019. http://www.xinhuanet.com/english/2019-11/15/c_138558369.htm.

YOO, JOHN. 2014. “The Legality of the National Security Agency’s Bulk Data Surveillance Programs.” *Harvard Journal of Law & Public Policy* 37 (3): 901–30. http://search.ebscohost.com.proxy.library.nyu.edu/login.aspx?direct=true&db=bth&AN=96403075&site=eds-live.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Vol. First edition. New York, NY: PublicAffairs.

http://search.ebscohost.com.proxy.library.nyu.edu/login.aspx?direct=true&db=nlebk&AN=1490460&site=ehost-live