

Surveillance in Digital Technology as a Threat To Democracy

Bana Nourkeyhani

Graduation Research Paper

Capilano University

April 23, 2018

LBST 490

Dr. Christopher Gratham

Introduction

The impressive rate at which digital forms of technology have been advancing over the past 20 years has placed us in an era unlike any other. As time has progressed and so have new types of digital technology, which are released so rapidly, the dangers and risks of these advancements have become increasingly more apparent. The world took a drastic turn for the worse following the events of the 9/11 attacks that took place in New York, killing thousands of civilians. Given this massive tragedy and threat to the American people, it was almost expected that the government would take extra steps to ensure the safety of its citizens. Although the event took place in the United States, the consequences of the actions of those that committed the crime have changed the ways in which we are surveilled on a day to day basis worldwide. Surveillance has been around for an indefinite amount of time; however, before the 20th-century surveillance was typically associated with espionage and traditional spying as a means of acquiring information. The evolution of surveillance with the progress of digital technology has altered the methods used to collect information as well as the intention and meaning of surveillance altogether. The original purpose of surveillance was to use it merely as a tool for monitoring. In spite of this, surveillance in digital technology is a threat to democracy as a result of the unexpected and abrupt evolution of these technologies; our privacy, autonomy, and democracy are being threatened. Additionally, as a result of the constant growing forms of mass surveillance, laws, and regulations are altering globally. Many people both in Canada and around the world are under the impression that mass surveillance is predominantly an American issue, when in fact it is international as a product of the Five Eyes, and it is far worse than anyone could have imagined. Laws are being used to further accessibility to citizen's personal

information via mass surveillance, and therefore, it is crucial to not only inform citizens but to also take it one step further by actively being engaged. Seeing that surveillance has wrapped humanity in an invisible net, this should not discourage people from being their true selves. If anything, these breaches of privacy that have intertwined within our justice system should motivate us to keep ourselves up to date and educated on the topic, and engage in conversation with others who may or may not be aware of what is going on. This paper will begin with an overview of what the definition of democracy is and how - in correlation with the description - it is under threat. Then, the role in which cyberspace and thus the internet plays in connecting digital technologies and surveillance will be considered to establish the connection between the two. In exploring both democracy and cyberspace, the definition and purpose of surveillance will be examined and applied to further sections throughout to demonstrate how it is a threat to democracy in more than one way. With these observations, the importance and lack of privacy, as well as the sudden expansion of social sorting, will be considered as a result of constant surveillance and how individualism and autonomy are becoming more challenging to obtain with democracy being under threat. Lastly, the Canadian government's role and involvement in mass surveillance via the Five Eyes, and Canada's anti-terrorism act(s) will be examined to demonstrate how these laws are threats to our democratic society in secrecy.

Research Methods and Research Questions

In approaching my graduation project, I was encouraged to narrow down my research question(s) as much as possible. Although I experienced great difficulty when I first attempted to do so, the more research I did, the more focused my vision became. After weeks and even

months of making an effort to find the question(s) that I want to address the most, I was finally successful and satisfied with my results. The two questions that I have chosen to answer are as follows:

- 1) How is surveillance in digital technology seen as a threat to democracy?
- 2) Is our democracy in Canada under threat as a result of surveillance in digital technology?

Upon doing my research on these topics, I became aware of how effortless it is to find information that is outdated. My research thesis is current and therefore continuously progressing, and the Canadian national security laws are still under debate, and thus as a result of this, I have come across many outdated sources. Despite this, it has been incredibly fascinating to read the evolution of surveillance since 2001, and even before with George Orwell's *1984*, and I have found that it has assisted me greatly in generating an accurate representation of its history. I used a vast variety of sources to ensure the absence of limitations for my sources. I acquired much of my information from credible and scholarly databases such as JSTOR and Google Scholar. The website for the Parliament of Canada provided me with an array of information regarding Canada's current and past national security laws. Most of the information that I gathered was acquired by a variety of books, which are all now a part of my personal library. The works of David Lyon (a Sociology Professor at Queen's University who specializes in Big Data and Surveillance Studies) have inspired me the most, followed by Glenn Greenwald (a renowned journalist for The Guardian Newspaper). I, therefore, did qualitative research, and I used literature reviews as well as a thematic analysis in hopes of answering my research questions as accurately as possible.

Critical Theory of Technology: Analysis and Placement

In preparation for beginning this research paper, I have reviewed Andrew Feenberg's *Critical Theory of Technology* to find one or two proper theoretical approaches that I identify with the most following technology. One of the most emphasized theories in Feenberg's work and one in which I can relate to is the Substantive Theory. This specific theory argues that the entire social world is being restructured and used as an object of control as a result of the new types of cultural system in which is being constituted by technology (Feenberg, 7).

Substantivism characterizes technology as an autonomous and valuable concept that can help to obtain the desired life and therefore does not view technology as neutral (Gratham, 22).

Although this theory has often been criticized as it grants absurd powers to technology, the more I research the topic, the less absurd and more relevant this theory seems to me in relation to my thesis. The Critical Theory approach presented by Feenberg is an intriguing theory which I have become familiar with early on in my University career. This theory views technology as an environment of struggle that has connected with this virtual battlefield in which political, social, and even personal matters are debated and criticized and therefore contribute to civilizational change (Feenberg, 12). New forms of oppression associated with modern industrialism are analyzed in this theory, and as a result, it emphasizes the need to modernize technology to contribute to the needs of a free society regardless of the new challenges societies might be facing (Feenberg, 11). Critical theory and Substantivism share an essential characteristic, and that is that they are both value-laden, and as a result of this I consider myself to be somewhere in between the two theories. The reason for my indecisiveness in choosing just one theory is because although I believe that technology is controlling the world with its unfathomable powers, I have hope that we can maintain control over these technologies.

Democracy

There is no conclusive definition of the term democracy, as the meaning of the word varies and is often determined by the individual or institution in question. Even though there are copious ways of defining democracy, there are characteristics that can connect the variety of interpretations, such as equality, and both political and individual freedom. In its original layout dating back to ancient Greece, democracy is a system of government meant to consist of power that is exercised with the consent of the people, voted by the people from within themselves. There are, of course, many different branches of democracy that have been altered and recreated throughout the decades. In the book titled *Strong Democracy: Participatory Politics for a New Age*, Benjamin R. Barber focuses on two forms of democracy: strong democracy and liberal “thin” democracy (Barber, xxxvi). Liberal democracy is outlined as the most dominant modern form of democracy that exists today and is rooted in premises about knowledge, human nature, and politics that are leaning more towards liberalism than democracy (Barber, 97). As well, thin democracy emphasizes the notion of individualism and implements an excess of political theory in liberalism, causing it to limit the role of democracy by undermining democratic structures and contributing to citizens lacking autonomy and individualism (Barber, 98). The most natural and accurate branch of democracy, which follows closely to its original design, is Strong Democracy. A strong democracy can be defined as a way of life; meaning that instead of delegating their power to a representative to be their voice, citizens govern themselves to the best of their ability as free individuals (Barber, 118). This form of democracy envisions politics as a way of living while seeing active citizenship as a way of life. “Effective dictatorships require great leaders;

effective democracies need great citizens” (Barber, p. xxxvi). Strong democracy does not rely on political leaders to survive, as it accomplishes a truly democratic society with competent and responsible citizens who re-establish the true meaning of democracy as individuals. This classification demonstrates how strong democracy can thrive and how liberal “thin” democracy cannot, as it lacks democratic characteristics and favours liberalism over democracy. Democracy is a way of life as opposed to merely just a political system orbiting around rules. It’s about the daily struggles of individuals who are striving to better their lives as well as themselves, and it is the only system that was initially built on the respect for an individual's search for justice, freedom, and autonomy (Barber, 128). Democracy encourages open-mindedness and thus as a result of this, citizens ought to defend it when it’s under threat. This specific analysis will be my definition of democracy moving forward in demonstrating how it’s under threat.

One of the most vital parts of what it means to live in a democracy is to know what the government in power is doing and to have the ability to question their decisions if need be (Lyon, 92). If citizens are unaware of the power that the state holds and thus subvert it, they are unable to approve of these powers being implemented and in turn defeating the purpose of democracy; this is a fundamentally dangerous threat that democracy faces. “Our capacity for justice makes democracy possible; but man’s inclination to injustice makes democracy necessary” (Niebuhr, 2011, p. xxxii). Since human beings appear to be the only species that are morally responsible, democracy is necessary to create a society with more freedom, liberty, and justice for all. Be that as it may, the balance of power between citizens and governments is shifting and becoming less focused on the elected and electorate and more on the ruling and the ruled (Poitras, Snowden, Citizenfour). With the rapid growth of power (as well as surveillance) comes the decline of

freedom, privacy, and autonomy within societies that label themselves as democratic states. Nowadays, the amount of personal information we share online is unprecedented and does not fit into previous models of understanding exactly how a democratic society should function (Hennig, 1). The fundamental understanding of how politics works is shifting at an alarming rate due to the evolution of technology, and thus, for proper regulations to be in place in a democratic society, we need to reevaluate our idea and understanding of what democracy is. Moving forward, we must proceed with this definition to ensure that it is functioning as it should be. In Canada, bills such as Bill C-51 and Bill C-59 are (partially) being introduced as an attempt to prevent terrorism in the country; however, in the midst of this effort, our democracy is severely under threat. With all of this taken into consideration, this does not mean that all forms of technology are considered a threat to democracy. The emergence of new forms of digital technology allows everyday citizens to communicate online with one another and creates more opportunity to reach an audience worldwide and this represents a democratization of communications generated by cyberspace (Deibert, 20).

Cyberspace and the Internet

Cyberspace is an unavoidable reality that has absorbed the globe in the complex skin of information and various forms of communication (Deibert, 11). It refers to an immersive environment that exists within the scope of the internet and is increasingly embedded in societies and communication forums and provides a safe space for people to vocalize without the immediate fear of discrimination. This environment has allowed two-thirds of the world to connect virtually at a remarkable speed; an unfathomable rate in which it has and continues to

spread (Deibert, 12). The reality of cyberspace is unavoidable; no one is immune no matter how hard they try. Even those who claim to be disconnected - in comparison to the average internet user - are still indirectly in contact with this form of “new” media (Deibert, 18). If you receive all of your local or international news via television news stations, the chances are that some (if not most) of the information that you’re being exposed to was obtained via the internet. The original designers of the internet “built a system of interconnection based on trust ... and how it might be abused was never predicted” (Deibert, 7). Since before the 21st-century we have never experienced being so dependant on and surrounded by large forms of technology, future generations will grow up relying on the internet and will live in a fragile and untrustworthy world (Deibert, 8). Given the quick evolution of cyberspace and the internet, it is inevitable that some governments use this as a tool for state control. States with authoritarian regimes - such as Iran - take advantage of the freedom provided by the internet as another excuse to assert control onto their citizens and thus gain control by decreasing the “freedom” aspect of “internet freedom” (Deibert, 18). However, it is not only authoritarian regimes and corrupt states that take advantage of cyberspace. American, Canadian, and European firms that used to pride themselves in their ability to connect people and wire the world together are now transforming those wires into tapped wires and secret weapons of war and repression without informing their citizens (Deibert, 20). This invasion exhibits how democracy is under threat as a result of the continuous growth of cyberspace and demonstrates the level of secrecy in said democracies. The core values of cyberspace must be discussed to ensure its security as a communication system for citizens, as we are at risk of degrading and destroying it (Deibert, 20). By having governments withhold the fact that they tap our communication wires via cyberspace from citizens, they are slowly but

surely stripping us of our privacy. The purpose of this environment is to communicate and speak freely without having to face significant discrimination, especially from the government of the country in which you reside. The fact that democratic states such as Canada have deemed it necessary to invade this space shows how privacy is being threatened as a result of surveillance via digital technology. Although the internet can distract users from aspects of the real and physical world, it cannot be seen as an autonomous realm, and mass surveillance demonstrates how the offline and online worlds are interconnected (Lyon, 42). Throughout the years, the internet has been transformed from a tool of democratization, into an ambiguous and unknown zone of mass surveillance (Greenwald, 120).

Surveillance

The nature of surveillance has altered excessively since the 9/11 attacks to the point where it does not only change the quality of our democracy, but it also modifies our capability of having control over the government as voters (Renzetti, 2015). Surveillance used to be defined as merely watching in the most literal way; with the constant growth of digital technologies, it has changed its focus to “seeing with data” (Lyon, 6). It has shifted its form into a tool used to keep track of virtually everyone regardless of their clean criminal and personal records (Poitras, Citizensfour). Surveillance could be defined as any systematic focus on personal information to control, manage, and influence those whose data is collected with a definitive purpose (Bennett et al. 7). It is primarily monitoring with the intention of intervention that often results in people being categorized in ways that lead to different groups of people being treated differently and targeted because of the category in which they’ve been placed in (Lyon, 109). Due to the

continuous growth in digital technologies and its availability, surveillance is no longer a matter of tracking people who are deemed as a threat. It has altered into a way of classifying people based on any personal data that is available; changing the idea of the target or threat from a person to a specific profile (Bennett et al. 8). This division has created a new term within itself called 'social sorting' which will be discussed in detail later on. Surveillance is all around us, everywhere we go. From your mobile device and laptop to your local grocery store's points card, local and international governments are constantly keeping tabs on citizens regardless of your past. Edward Snowden, who was a former National Security Agency (NSA) and the Central Intelligence Agency (CIA) employee, gained popularity as a result of him leaking and exposing confidential NSA documents, while most of the world was unaware of the severity of mass surveillance. Countries such as Germany were appalled when it was revealed that Chancellor Angela Merkel's cell phone was targeted by the NSA for years, causing an uproar globally (Greenwald, 141).

The American government implemented the Patriot Act in 2001 following the 9/11 attacks, which indirectly inspired countries worldwide to apply similar laws. Since the start of the Cold War in 1946, the countries that have been the most hyper-aware and active in this realm are the countries in the Five Eyes (FVEY): Canada, The United Kingdom, Australia, New Zealand, and The United States. Once Snowden bestowed his files onto trusted journalists (such as Glenn Greenwald), anti-terrorism laws began to slowly resurface particularly in these five countries as they collaborated with the NSA (Lyon, 59). Canada's national security laws began to alter at almost the same rate as the U.S; in the absolute secrecy of course. The FVEY will be discussed further in the section titled *The Five Eyes* followed by *Bill C-51* and *Bill C-59* which will

observe the section titled *Canada's National Security Laws* to demonstrate how these laws use surveillance as a tool and therefore are a threat to democracy.

Privacy

With the developments that have transpired in technology in the past century, privacy and freedom have been combined into one term which is simply referred to as privacy. Privacy is connected with living in a democratic society; a place where we are free to disagree with the government when necessary without being fearful of the consequences and having limits on what the governments can keep hidden from everyday citizens (Lyon, 11). Privacy is a well established human right that is frequently seen as having multiple dimensions such as territorial privacy, personhood, the control of personal information, intimacy, and the choice to be left alone. It is a pivotal concept that helps to shed light on what is wrong with mass surveillance; mass surveillance that violates rights such as freedom of speech, association, religion and other such rights that are basic to democratic ways of organizing society (Lyon, 92). Not only does privacy matter as a vital value in itself but it is also essential for practices such as democracy that supports privacy (Lyon, 93). With the continuous growth of power and surveillance comes the decline of privacy and autonomy within a democratic state. Invading the privacy of citizens should be an arduous task to accomplish, as it is incredibly intrusive. "Privacy is the core condition of being a free person" (Greenwald, 172). For any person to be a free individual, privacy is necessary for personal autonomy to be obtained. It is only when we believe that no one is watching us do what makes us feel free that we feel safe enough to truly explore what it means to be ourselves (Poitras, Snowden, Citizenfour). What makes the internet so unique is that it

presents us with the ability to speak and act anonymously, as if nobody else is watching, which is vital to individual exploration (Greenwald, 174). Taking privacy away from citizens is an immeasurable and disturbing reality that is a massive threat to both democracy and our autonomy. Edward Snowden revealed, and continues to do so via trusted journalists, NSA documents that prove we are always being watched by the NSA as well as other government organizations (Poitras, Citizenfour). Society is gradually realizing that our constant surveillance is constraining the boundaries and limitations of intellectual freedom and explorations for individuals. Privacy is a part of the common good and is an essential component of democracy as well as of decent human life (Lyon, 12). A society in which the private realm is eliminated, and everyone knows that at any moment they can be watched by the state is a society that has lost its character and unique features on an individual level as well as a societal level (Greenwald, 174).

Many people believe that there is no harm in being watched by the government as they assume that they are not doing anything wrong, as the only people that have anything to be worried about are those engaged in criminal activity (Greenwald). This mentality is grounded in the assumption that there are only good and bad people in the world and therefore good people are not involved in bad behaviour and thus have nothing to hide. Regardless of the severity of what it is we are protecting, everyone has something to hide from a particular audience that they wish to conceal specific truths. Although people may claim that having the government surveil their lives isn't a breach of privacy and that privacy does not matter to them, their actions indicate otherwise (Greenwald). During a TED talk given by Glenn Greenwald on the topic of why privacy matters, Greenwald highlights the hypocrisy seen within the groups of individuals who devalue themselves as harmless beings by claiming that privacy does not matter. "People

may say that privacy doesn't matter to them, but their actions negate the authenticity of that belief" (Greenwald). He continues by merely demonstrating that although people may say that this is their opinion, they take many steps to ensure their private realm is not being compromised by taking actions such as purely locking their doors (Greenwald). With the existence of Canada's current security laws that resemble the United States' anti-terrorism act which revolves around collecting information via surveillance, our privacy is undermined persistently. When we are aware of the fact that we are being watched, our behaviour changes dramatically, and therefore we are unable to be our true autonomous selves. Everyone in all societies shares the desire for privacy, as it is an essential part of what it is to be a human being and that is under threat with the existence of mass surveillance, and that is why privacy matters; it is an essential component to being a human being.

Social Sorting

A concept coined by David Lyon, social sorting is primarily what today's surveillance achieves by separating one group from the other (Bauman & Lyon, 13). Surveillance is virtually a means of social sorting generated by collecting data via digital technology which enables trends to be found based off of the information being collected and thus creating a pattern that leads to cynical discrimination between different groups of people. This division results in one group being treated differently from another and targeting primarily population groups before individuals (Lyon, 101). Despite the fact that the expression was conceived post 9/11 as a result of surveillance, social sorting has been seen in many societies as far back as the 17th century when slavery was first known to have occurred. During that time, individuals were separated

based on the colour of their skin, class, and gender; beaten and taken advantage of as a result. While slavery still -covertly- exists in both developed and undeveloped states, social sorting has evolved and is evident through surveillance. Before surveillance - especially mass surveillance - became prominent, it had begun moving towards the direction of systematic social sorting long before the functions of surveillance focused its attention on profiling specific groups of people (Lyon, 38). Trends in surveillance have solidified further since 2001, and social sorting is even more evident now than before. Debates over racial profiling have become more prominent, and therefore such classifications frequently occur by way of human observers (Lyon, 145). The evolution of technology has made social sorting far more influential and potent as it has now intertwined computer assistance into the process. Individuals falling into the wrong category as a consequence of social sorting have their reputation and future opportunities made vulnerable by these surveillant profiling systems that have been made more accessible as a consequence of digital technologies. (Bauman and Lyon, 130). Alongside, proving one's innocence has become much more difficult for those who happen to fall under these categories, as they are considered guilty until proven otherwise by the system which is surveilling the individual, to begin with (Bennett et al. 12). Groups that are marginalized are susceptible to risks as desirable forms of security that are available to other citizens are not offered to them; excluding them from the opportunity of participating in society (Bennett et al. 47). This social separation defeats the purpose of democracy as it excludes certain individuals solely based on their race which has been deemed dangerous and, in turn, does not allow them to be active members of society. Not only is surveillance a matter of personal privacy and social sorting, but it is also a matter of social justice. This division is more conspicuous in the United States as a result of information

leaked by whistleblowers as well as media coverage; however, social sorting is in full effect in Canada.

Canada's Role in Mass Surveillance

Five Eyes (FVEY)

For my second research question, I wanted to focus on Canada's role in regards to surveillance. Other than the fact that I am a Canadian, I decided to do this because most of the aspects we hear concerning this issue usually come from the U.S or the U.K., while Canada is regarded as a perfect nation with a handsome Prime Minister. Once I began my research, the first thing that I came across was the Five Eyes, also known as FVEY. The Five Eyes alliance started initially as a part of a secret treaty in 1941 between the United Kingdom and the United States of America; however, as the cold war intensified, three more countries were added in the 1950's: Australia, Canada, and New Zealand (Lyon, 58). This alliance has ensured that the net of surveillance is cast globally, and thus, as Edward Snowden communicated through his manifesto in 2013, they have imposed a system of secret surveillance around the world for which there is no asylum (Greenwald, 23). The mass surveillance that takes place within the FVEY is initiated by the NSA, the most substantial intelligence agency in the world who conducts most of its surveillance work through FVEY, and all of the countries involved are subject to this as well (Lyon, 57). The members of this alliance, however, are not the only ones that are subject to this. Their allied countries - such as Germany and Brazil - as well as countries deemed unfriendly by the US - such as Russia and China - are also subject to this mass surveillance initiated by the

NSA (57). In some of the documents released by Snowden in 2013, they revealed that the CSE (Canada's version of the U.S national security agency) had collaborated with the NSA significantly (Deibert, 259). This coordinated partnership can be seen in instances such as when the CSE allowed the NSA to use the U.S embassy in Ottawa, Ontario as a base for espionage during the G8 and G20 summit meetings in 2010 (Lyon, 59). Canada is an active partner with the NSA as well as a dynamic surveillance force of its own, making it one of the first countries from the Five Eyes to sustain the impact of its mass surveillance (Greenwald, 119). This influence is apparent in other instances that are less evident such as how Canada's internet routing goes through the U.S first and thus making it susceptible to interception by the NSA (Lyon, 59). The relationship between the countries in the Five Eyes alliance is exceedingly close, and as a result of this, the NSA's desires are put above the privacy of the citizens of each state (Greenwald, 122). The reliance put onto the U.S infrastructure and the NSA by Canada particularly severely compromises Canadian sovereignty and therefore the privacy rights of Canadian citizens (Lyon, 60). The relationship between the NSA and Canada's involvement as an active member of the Five Eyes contribute to how we see surveillance as a threat to our democracy.

Canada's National Security Laws

The Canadian government was fast to implement an anti-terrorist act following the attacks of 9/11. Less than two months after the Patriot Act was signed into law by George Bush, the Canadian Liberal government passed Bill C-36, the Anti-Terrorism Act (Deibert, 255). This act gave law enforcement and intelligence agencies new capabilities, as well as providing CSEC new international powers among other things (Deibert, 255). It wasn't until Edward Snowden

leaked CIA and NSA classified files, and the shooting on Parliament Hill in 2014, that Canada began to upgrade its Anti-Terrorism act. Roughly 14 years after the implementation of the American Patriot act of 2001 and Canada's own Bill C-36, Stephen Harper's right-winged government proposed Bill C-51; a bill that is almost on par with its southern neighbours governance in regards to the issue. Both the Patriot Act and Bill C-51 - and potentially Bill C-59 - contribute to, and implement, the ongoing threat to democracy that is social sorting and the invasion of privacy.

Bill C-51 - Anti-Terrorism Act, 2015

In January 2015, Stephen Harper's government proposed Bill C-51 - Anti-Terrorism Act. When this bill came out, there was an uproar and many protests by people who were enraged; protests that continue to this day (McDermott). When asked about his opinion on the Anti-Terrorism Act during a conference at Ryerson University in 2015, Edward Snowden said - via Skype - that Bill C-51 "fundamentally changes the balance of power between the citizen and the state" (Snowden). This bill gives expanded powers to CSIS, an intelligence agency that was created intentionally to separate spying from policing, that allows it to collect and share personal information about Canadians with other departments and agencies (Kimantas, 11). Although the purpose of CSIS was to separate policing from intelligence gathering, this bill grants CSIS with policing powers, which is a ruthless anti-democratic move. As a result of this, CSIS will be allowed to violate citizens' charter of rights by merely obtaining warrants during secret hearings that allow for this to happen (Kimantas, 11). When talking about this bill once the Senate passed it,, the leader of the Green Party, Elizabeth May, emphasized that this bill is more about creating

secret police than it is about terrorism; calling Bill C-51 the death of freedom in Canada (Kimantas, 11). The stakes for democracy are high with this bill, as it puts a chill on many kinds of freedom of speech and criminalizes speech acts that have no connection to acts of violence (McDermott). The CBA (Canadian Bar Association) commented on the bill, saying that the language of the legislation is vague. As a result of this, it wouldn't improve the safety of Canadians, contrary to what was publically stated by Harper's government in regards to the implementation of the bill (The Real Threat is C-51, 2015). Instead, this would limit freedoms and liberties for Canadians. This bill also allows court judges to restrict all sorts of charter rights without any democratic discussion whatsoever (Forcese, 2017). As well, this bill also authorizes government institutions - such as Canada Revenue Agency - to share personal information with the RCMP without the consent or knowledge of citizens (McDermott). With the implementation of Bill C-51, CSIS powers have increased in ways that are ill-defined to a basic understanding of what constitutes a free and democratic society, deeming it a threat to our democracy in Canada.

Bill C-59 - National Security Act

Proposed by Justin Trudeau's Liberal Government in 2016, bill C-59 is still under debate in the house of commons, and changes won't come until the Senate passes the bill. The purpose of this bill, as set out by the Liberal government, is to fix issues caused by Bill C-51. Instead, it adjusts specific problems but fails to correct others while also creating new ones (McPhail & Gill, 2017). Bill C-59 is set to constrain and soften some of the disruptive powers given to CSIS, but, in turn, creates an entirely new act for CSE - Canada's signals intelligence and cybersecurity agency (McDermott). This bill grants CSE the power to conduct secret hacking, which is a step

backward for our security in Canada (McPhail & Gill, 2017). Although Bill C-59 is more charter compliant, the creation of a separate law for CSE is the most significant issue with this bill, as the powers given to CSE would be a tremendous threat to our democracy (McDermott). There is a great deal of oversight that comes with this bill, which isn't necessarily a bad thing. However, counterbalancing that is the actuality that the thresholds for collecting information have lowered. Currently, CSE only obtains information if it's necessary and relevant, but if this bill passes, CSE will be granted the ability to gather a substantial amount of information; more than they are already collecting (McDermott). Bill C-59 also creates new frameworks for mass data collection within Canada and would allow CSE and CSIS not only to obtain information about Canadians but also to use the information collected as long as it is publically available (McPhail & Gill, 2017). The government has yet to explain how the collection of this information via mass surveillance would be necessary for protecting those living in Canada. If Bill C-59 passes without further improvement, it would not only be a massive threat to our democracy; it would also impact our human rights. Although Bill C-59 fills a crucial gap in Bill C-51 by improving oversight and accountability for our spy agencies, it creates a range of troubling new powers for CSIS and especially CSE (McSorley, 39). Alongside, it fails to address long-term problems in Canadian national security law and continues to use vague terms in the charter which makes it easier for these intelligence agencies to collect data via mass surveillance (Canadian Civil Liberties Association, 2017).

Conclusion

Having discussed and observed ways that surveillance in digital technology is a threat to democracy, it is easy to be taken back by technology and want to change the relationship we share with it. Alas, we should not allow this to discourage us and alter our behaviour. “If we change our behaviour because a government agency somewhere is doing the wrong thing ... if we sacrifice our values because we were afraid, we don’t care about those values very much” (Snowden). Instead, we, as global citizens, need to be more engaged, educate ourselves and each other and speak out when the time is right. By creating a climate which standardizes these types of activities, as Canadians, we’re accepting that we think that these types of operations are acceptable when they’re not (The Toronto Star, 2017). These operations threaten our democracy, privacy, autonomy, and individuality. As Canadian citizens living in a democratic society, we need to be active and keep in mind that although Stephen Harper is no longer in office and the Liberals are now in charge, the issue of mass surveillance is not over and still very much a threat to our democracy. Lastly, many people currently believe that these are not issues solely because they do not engage in criminal activity. As Glenn Greenwald said in regards to why privacy matters, “we can try to render the chains of mass surveillance invisible or undetectable, but the constraints that it imposes on us do not become any less potent” (Greenwald).

Works Cited

Barber, Benjamin R. *Strong Democracy: Participatory Politics for a New Age*. University of California Press, 2009.

Bennett, Colin J., et al. *Transparent Lives: Surveillance in Canada*. Athabasca University Press, 2014.

Bauman, Zygmunt; Lyon, David. *Liquid Surveillance*. Polity Press, 2013.

Citizenfour. Dir. Laura Poitras. Perfs. Edward Snowden, and Glenn Greenwald. Radius-TWC. 2014. Documentary Film.

Deibert, Ronald J. *Black code: surveillance, privacy, and the dark side of the internet*. McClelland et Stewart, 2013.

“Edward Snowden comments on Bill C-51 and Canadian liberties.” *YouTube*, uploaded by CBC News, 4 March 2015,

<https://www.youtube.com/watch?v=Z31r4MfBvd8&t=58s>

Forcese, Craig; Roach, Kent. “Bill C-51: The Good, The Bad, ... And The Truly Ugly.” *The Walrus*. 4 May 2017, p.1.

<https://thewalrus.ca/bill-c-51-the-good-the-bad-and-the-truly-ugly/>

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S surveillance state*. New York, NY: Picador. 2015. Print.

Greenwald, Glenn. “Why Privacy Matters.” TED. Oct. 2014.. Lecture.

Kimantas, Janet. "C-51'S Criminalization of Caring." *Alternatives Journal (AJ) - Canada's Environmental Voice*, vol. 41, no. 3, May 2015, p. 11. EBSCOhost,

ezproxy.capilanou.ca/login?url=https://search-ebSCOhost-com.ezproxy.capilanou.ca/login.aspx?direct=true&db=a9h&AN=103367842&site=eds-live&scope=site.

LastWeekTonight. "Government Surveillance: Last Week Tonight with John Oliver (HBO)."

YouTube. YouTube, 05

Apr. 2015. Web. 23 Apr. 2017.

Lyon, David. *Surveillance After September 11*, Polity Press, 2003.

Lyon, David. *Surveillance after Snowden*. Polity Press, 2015.

McDermott, Meghan. Discussing Bill C-59, Capilano Students' Union, 19 March 2018, Capilano University, North Vancouver, BC. Guest Lecture.

Mcsorley, Tim. "It's Better Than C-51, but That Isn't Saying Much: Five Reasons Civil Liberties Advocates Are Worried about the Liberal Government's Security Policy Redo." *CCPA Monitor*, vol. 24, no. 4, Nov/Dec2017,

pp. 39-42. EBSCOhost,

ezproxy.capilanou.ca/login?url=https://search-ebSCOhost-com.ezproxy.capilanou.ca/login.aspx?direct=true&db=a9h&AN=126094610&site=eds-live&scope=site.

McPhail, Brenda; Gill, Lex. "Five Questions Mps Must Ask about Bill C-59." *The Toronto Star (Toronto, Ontario)*,

2017. EBSCOhost,

ezproxy.capilanou.ca/login?url=https://search-ebSCOhost-com.ezproxy.capilanou.ca/login.aspx?direct=true&db=edsgin&AN=edsgcl.515470791&site=eds-live&scope=site.

"New Spy Powers Must Be Debated; Bill C-59." *The Toronto Star (Toronto, Ontario)*, 2017.

EBSCOhost,

ezproxy.capilanou.ca/login?url=https://search-ebSCOhost-com.ezproxy.capilanou.ca/login.aspx?direct=true&db=edsgin&AN=edsgcl.520717017&site=eds-live&scope=site.

Niebuhr, Reinhold. *The Children Of Light And The Children Of Darkness: A Vindication Of Democracy And A Critique Of Its Traditional Defense*. The University of Chicago Press, 2011.

Renzetti, Elizabeth. "Snowden's message to citizens: Democracy itself is threatened." *The Globe and Mail*. The Globe and Mail. 20 Feb. 2015.

www.theglobeandmail.com/opinion/snowdens-message-to-citizens-democracy-itself-is-threatened/article23138430/?arc404=true.

"The Real Threat is C-51." *Aboriginal Multi-media society*, Apr. 2015, p. 5.

"The Relationship Between Bill C-51 and Bill C-59." *Canadian Civil Liberties Association*. 12 September 2017. p.1. <https://ccla.org/relationship-bill-c-59-bill-c-51/>

Trew, Stuart. "What is C-51 for?" *CCPA, NDA*, p.3.