# Digital Surveillance in the Post-Snowden Era

Jessica Percy Campbell

A Thesis

In

The Department

Of

Sociology and Anthropology

Presented in Partial Fulfillment of the Requirements

for the Degree of Master of Arts (Sociology) at Concordia University

Montreal, Quebec, Canada

December 2016

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: Jessica Percy Campbell

Entitled: Digital Surveillance in the Post-Snowden Era

and submitted in partial fulfillment of the requirements for the degree of

Master of Arts (Sociology)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Chair

Dr. Jean-Phillipe Warren

_____ Examiner

Dr. Orit Halpern

_____ Examiner

Dr. Martin French

_____ Supervisor

Dr. Beverley Best

Approved by Dr. Jean-Phillipe Warren

Chair of Department

_____

Dean of Faculty

Date _____

## Abstract

Since 2013, we have learned a great deal about the inner workings of the surveillance state of the U.S. and its allies in the Five Eyes (Canada, New Zealand, the UK, and Australia). Through Edward Snowden's leaks to the press, hundreds of classified National Security Agency (NSA) documents have been made available to the public online. Perhaps most importantly, the Snowden leaks have uncovered relationships between the corporate empire of digital communications platforms and Western intelligence agencies. For example, one internal NSA document demonstrates that Silicon Valley giants such as Google, Facebook, Apple, Yahoo, Microsoft and Skype have shared access to their servers with the NSA through the PRISM program for almost a decade. PRISM and related programs have allowed the Five Eyes to collect and store unprecedented troves of information on their own citizens, including massive amounts of e-mails, text messages, online chats, status updates, phone calls, videos, cellphone location data and search engine history despite constitutional protections against unwarranted searches. As state-run initiatives collect personal data on hundreds of millions of people on an untargeted basis, this thesis questions the scope of their reach in the U.S. and Canada. Has increased public awareness resulted in significant policy reform or have intelligence agencies and corporations continued running the same patterns? This work questions the future of the internet and digital privacy as various entities collect user data for the ultimate purpose of predicting and manipulating user behaviour, both online and in "real life". As we enter unchartered realms of technological capability, the use of strong encryption and alternative software programs are offered as temporary solutions for securing communications online.

*Keywords*: Big Data, predictive analytics, Snowden, surveillance, predictive policing, surveillance capitalism, datafication, encryption

**Acknowledgements**

My sincerest gratitude goes out to the four interview participants who have greatly informed and encouraged this thesis. Without your technological and legal expertise, this project could not exist. Thank you all for your hard work and for the intriguing conversations.

I would also like to acknowledge my brilliant MA cohort, my best friend Lindz, and my partner Wes. I could not have asked for a more talented group of people to surround myself with. Thank you for the late nights, the laughs, and the unwavering support (both academically and personally) over the last few years.

And finally, to my committee, Dr. Best, Dr. French, and Dr. Halpern, who allowed my creative process to flourish without micromanagement, arbitrary deadlines, or useless meetings. Thank you for being enthusiastic about my work and inspiring through your own.

**Table of Contents**

# Introduction

As digital communication technologies become increasingly popular and accessible across the globe, various organizations have been quietly collecting and storing unprecedented amounts of personal information from its users. Put simply, two major motivations guide data collection programs, “one for intelligence, the other for money” (Wasserman, 2015:15). As a result, run-of-the-mill internet activities such as personal e-mails, Google searches and private Facebook messages are being simultaneously commodified by corporate actors (Zuboff, 2015) and intercepted by government intelligence agencies (Schneier, 2015; Greenwald, 2014; Fuchs, 2014). As revealed by the now-famous National Security Agency (NSA) contractor, Edward Snowden, the personal communications of hundreds of millions of internet users around the world are being collected and stored by their own governments. Evidently, the NSA’s post 9/11 strategy to “collect it all” (Greenwald, 2014:89) employs untargeted-surveillance programs to scrape as much user information from the web as possible. As of 2012, billions of text messages, e-mails, phone records, search engine history and location data, were being processed by the NSA on a daily basis through various programs (Greenwald, 2014; Schneier, 2015; Goldfarb, 2015). According to Geist & Wark, these findings serve as tangible evidence of what digital privacy advocates had suspected for years, “that fears of all-encompassing network surveillance and data capture that were envisioned as worst-case scenarios have become a reality” (Geist & Wark, 2014:1).

Further, Snowden’s leaks revealed that the NSA had publicly lied to Congress about the capabilities of these programs on numerous occasions. In a 2012 congressional hearing, when NSA Director Keith Alexander was asked whether the NSA collected data on US citizens, he issued the following statement: "we’re not authorized to do it nor do we do it" (Cate, 2015). Likewise, a few

months before Snowden's initial disclosures, Senator Roy Wyden asked James Clapper, the Director of National Intelligence (DNI) the following question: "Does the NSA collect data on millions, or hundreds of millions of Americans", to which he responded "No sir... not wittingly" (Wyden, 2013). Despite the overwhelming evidence rendering these claims blatantly false since the Snowden revelations, Clapper has yet to be reprimanded. As articulated by a member of the US Homeland Security Council, "I am still waiting for the attorney general to indict him for a clear-cut case of perjury" (Hamilton, 2015:47). Snowden, on the other hand, faces a potential sentence of 30 years in prison under the Espionage Act should he choose to return to the United States (MacAskill, 2015).

Still, these disclosures have resulted in fierce political debates surrounding state surveillance and individual privacy rights (Fidler, 2015), further classified by Laura Lynch as "a vigorous and sustained discussion about security, privacy and the citizen's right to know in the United States and around the world" (Lynch, 2016:15:05). Out of the tens of thousands of classified NSA documents Snowden passed along to Glenn Greenwald, the public only has access to the few hundred that have been released through *The Guardian* and other media outlets. They have also been made available online through the Snowden Archives. As leaked documents continue to be released, we have gained significant insight into the surveillance industrial complex, which traditionally operates behind a thick wall of secrecy. The released documents revealed some of the secret ways in which the Five Eyes (FVEY), (US, Canada, New Zealand, Australia, the U.K,) and their loosely affiliated partners (such as the Netherlands, Norway and Sweden) work together to secretly collect and share massive amounts of digital data on their own citizens and foreigners alike (Fidler, 2015).

The information disclosed pertains to secret court rulings concerning the scope of NSA surveillance, internal briefing documents outlining the capabilities of many data-mining programs, and breaches of international law by intelligence agencies in the Five Eyes. Civilians aren't the only targets of these programs, as the documents also demonstrate the NSA has spied on the communications of government officials and world leaders of allied countries including German chancellor Angela Merkel (Ball, 2013b). They have also used spy programs to target humanitarian non-profits like UNICEF, the World Health Organization (WHO) as well as the offices of the United Nations (Ball & Hopkins, 2013). Other documents show that Canada's Communications Security Establishment (CSEC) have been collecting the location data of Canadians who log on to airport Wi-Fi for weeks after visiting the airport, as part of a trial experiment for the NSA. Under this program, the CSE also gained retroactive access to cellphone data generated in the weeks leading up to visiting the airport (Wetson, Greenwald & Gallagher, 2014).

Due to the lack of transparency within intelligence agencies as well as internet corporations, the fine points of mass surveillance can be challenging to investigate. Without whistleblowers like Edward Snowden or AT&T technician Mark Klein who alerted the public about a secret NSA data collection splitter room in AT&T's San Francisco office years' prior, some government surveillance tactics have been speculated on but never confirmed with tangible evidence. Intelligence programs operate under their own secret laws and secret courts such as the Foreign Intelligence Surveillance Court (FISC) in the United States. Because of their confidential nature, their programs and the rulings that pertain to them are kept private and are not typically subject to congressional debate or public scrutiny. The joint efforts of the Canadian Security Intelligence Service (CSIS) and Communications Security Establishment (CSE) are even less transparent in Canada, as they operate without an external oversight board. In the words of

University of Toronto professor Ron Deibert: "The Canadian checks and balances just aren't there. We have no parliamentary oversight of CSE, no adequate independent entity to watch the watchers and act as a constraint on misbehaviour. It just doesn't exist now" (Geist, 2015:228-229). In an interview with Canadian Journalists for Free Expression (CJFE), Snowden cautioned that the surveillance state may only be getting stronger in Canada:

> Canadian intelligence has one of the weakest oversight frameworks out of any western intelligence agencies in the world and when they're trying to expand their powers, you know it's pretty amazing that we have the Canadian government trying to block the testimony of former Prime Ministers who have had access to classified information…who are warning the public broadly saying 'this is something we really need to talk about, this is something we really need to debate, this is something we really need to be careful about' (CBC News, 2015: 0:02-:034).

On the topic of expanding powers, Geist has also argued that since Snowden, recent Canadian legislation has "adopt[ed] lower thresholds for standard warrants" through Bill C-13 as well as "expand[ed] information sharing" and policing power of Canadian intelligence and the RCMP through Bill C-51 (Geist, 2015:226). Furthermore, Geist argues that new trade deals such as the Trans Pacific Partnership (TPP) threaten Canadian privacy rights as well:

> The TPP features several anti-privacy measures that would restrict the ability of governments to establish safeguards over sensitive information such as financial and health data as well as information hosted by social media services… As countries begin to embrace restrictions on data transfers solely to countries with adequate privacy protections, the TPP could restrict the ability of the 12 member countries to do so (Geist, 2015a).

While the datafication of society continues to expand, and circumscribe our social, political and educational experiences, the implications of data mining become a highly significant area for research and inquiry. Ubiquitous surveillance performed for intelligence, law enforcement and commercial gain is shaping both the future of the internet and democracy as we know it. If political sociology is to reflect on contemporary power dynamics between democratic states and citizens,

then government surveillance should be a core focus of study within the discipline. As will be explored in the literature review section of this paper, Christian Fuchs has shown how theorizing surveillance from a Marxist perspective can help to untangle the relationships between big business and government in the digital world (2014). Alongside Shoshana Zuboff's theory of "surveillance capitalism" (2015, 2016), which elaborates on massive scale data collection for the sake of profit under the Google empire, this paper utilizes Fuchs' perspective to explore invasive government and corporate surveillance efforts as well as counter initiatives that subvert them.

Snowden's whistle-blowing has served to reengage a public debate over internet control and privacy rights that has been ongoing since the 90s. However, further awareness and activism is still needed to reduce the various ways internet users are exploited in the information age. The purpose of this work is to help raise awareness through the critique of blanket surveillance programs in the post-Snowden era. This thesis explores the question of whether significant changes have taken place in the surveillance states of US and Canada since Snowden made his public debut in June of 2013. Here, changes can be achieved through official channels via policy or legal reform. They can also be made possible through corporate initiatives such as non-compliance with the government or promoting applications that use encryption by default. Alternatively, change can also come from internet users, which may avoid certain programs or take extra steps to secure or obfuscate their data (Brunton & Nissenbaum, 2015).

In order to deepen the investigation of Western surveillance from a critical sociological perspective, this work utilizes a wide variety of sources including the Snowden documents themselves, subsequent journalistic reporting from Greenwald and others from 2013-2016, interview videos from Snowden himself, and academic work by experts in the field of law, digital

studies, cryptography and surveillance. Because the Snowden story is ongoing, this work can be considered as part of the first wave of scholarly work using these resources. My investigation has also been guided by four semi-structured interviews with relevant researchers in the Montreal area. The purpose of this study is to add to the academic discussion on digital privacy, security, and civil liberty as we grapple with the new challenges and opportunities made possible by budding computer technologies and the corporatization of the web. If sociology is to stay relevant and on top of current affairs, there is a need for a critical account of this story and its subsequent outcomes. My goal is to contribute to that effort. The outline of this project proceeds as follows: Chapter One consists of a brief overview of the literature and methodology used to inform this writing; Chapter Two: The Robin Hood of the Information Age, explains Snowden's motivations in his life-changing decision to leak an unprecedented amount of classified documents to the press; Chapter Three: Intelligence Programs, Effectiveness, Exploitation and Legality, dives deeper into the capabilities of civilian spy programs, the policies that protect them and their general effectiveness; Chapter Four: Activism and Encryption, looks for solutions to digital privacy invasion by elaborating on alternative strategies for secure communications. Chapter Five: Social Change, concludes with thoughts on the unequal distribution of risk associated with modernized surveillance tactics alongside the future of the internet and predictive analytics.

# Chapter One

## Literature Review and Methods

This chapter reviews relevant literature on internet surveillance as well as the aftermath of the Snowden documents. Much of the literature referenced here sheds light on the data surveillance culture of companies such as Facebook and Google, and outlines their motivations for setting up business models in this way. Understanding the corporate side of the web is useful for understanding how law enforcement and intelligence agencies gained access to the data they have today. For example, if those companies had not relied on the collection and sale of user data as their primary modes of profit, or if they had nothing to share with intelligence agencies, the surveillance capabilities of the NSA would be gravely weakened. Moreover, this review sheds light on the Snowden revelations as a crucial component to debates on several political topics, including freedom of the press, journalism ethics, whistleblower rights, the future of the internet, as well as surveillance states at large. Although much of the significant scholarly discussion surrounding this topic has been written before 2013, these works can still be used effectively to theorize or explain what we now know is happening behind closed doors of the Western intelligence community, as well as with the corporatization of the web.

David Lyon, a known expert in surveillance studies, is helpful for explaining what exactly the Snowden documents mean for democracy. In his 2015 article, “The Snowden Stakes”, Lyon insists the future of the internet is the most important question raised by these disclosures: "If there is a key issue raised by the Snowden revelations, it is the future of the internet. Information and its central conduits have become an unprecedented arena of political struggle, centered on surveillance and privacy. And those concepts themselves require rethinking" (2015:139). Due to

the public's general lack of knowledge about government and corporate surveillance over the past four decades, Lyon calls for fresh and accessible research that accurately reflects the new data collection capabilities that come along with new ways of communicating online. In the contemporary context, more research is needed on everyday social media practices such as the circumstances under which users share data and with whom. The analyses of bulk surveillance practices are fundamental to the future of digital communications and human rights to privacy and free speech (Lyon, 2015). However, even though inner workings of surveillance are notoriously elusive and difficult to capture, the limited information we have about secretive intelligence programs is enough to form a baseline critique. Lyon coins the term "liquid surveillance" to capture its omnipresence in today's culture of smartphones and data mining:

> Surveillance is no longer highly specific and [is] going down very discrete conduits, it's flowing everywhere. It flows within organizations, it's everywhere. Personal data especially flows within and between organizations in unprecedented ways and so there's less of an obvious relationship going on. It becomes very fluid and moveable…therefore, it becomes quite difficult to know where those personal data are flowing if something that began in a commercial context, consumer surveillance, ends up going through data brokers and is being used for policing or government purposes, you don't know where it's gone (Council of Europe, 2016, 0:39).

Here, the boundaries between state surveillance and corporate data mining have blurred, as subcontracted security and tech companies work together with government intelligence agencies in Western countries. Making reference to his previous work, Lyon stipulates that a loose network of government authority and technical professionals have created a complex surveillance community. Data collection methods previously reserved for military personnel are now being used by an increasing number of agencies. As a result, it becomes difficult for outsiders to tell who exactly is conducting mass or targeted surveillance (Bauman in Lyon, F2015). For Lyon, "The Snowden Stakes" are high, shining a new spotlight on age old questions of human rights and

freedoms: “The revelations have rightly remained buoyant in the headlines, just because so much is ‘at stake’ not merely for Surveillance Studies or the future of the internet, but more significantly**,** for privacy, human rights, civil liberties, freedom and justice" (2015:144).

Lyon notes that clumsy metaphors for explaining data storage and movements are detrimental to policy reform as well as active discussion (2015). He explains that while ‘the cloud’ is an expression used to refer to online data storage, the physical locality of data and the way it flows is important for critical discourse on the infrastructure of the Internet (Lyon, 2015:145). Likewise, Clement and Obar insist that the metaphor of the cloud obstructs effective political discussion about surveillance, as the physicality of what is actually happening is rarely discussed or even understood (2014). The idea of data invisibly floating through the air gives it a mystical quality which makes it difficult to pin down in terms of legal boundaries. This makes it harder to subject data flows to territorial laws (Clement & Obar, 2014). Lyon (2015) and Clement and Obar (2014) have both argued that the precision of metaphorical language can be crucial to progressive discussions around policy formation and legal decisions surrounding Big Social Data. Thinking about data as physical matter that flows through fiber-optic cables in data packets helps us to compare online messages to letters in the mail. This makes it easier to discuss what is happening to digital data as it flows through cyberspace. Letting go of the ‘cloud’ metaphor becomes important when discussing major issues surrounding constitutional protections when data crosses national borders. Once online data leaves one country and travels through another, the user who generated the data no longer enjoys their home country’s constitutional rights to privacy. Currently, even efforts to keep data localized are being subverted by new international trade deals. For example, Geist explains how the TPP threatens to reverse recent Canadian initiatives to keep sensitive data within the country in response to US surveillance: “provinces such as British

Columbia and Nova Scotia have enacted laws to keep government information (such as health data) within the country. The TPP is designed to counter these efforts by restricting the ability of governments to mandate local data storage" (Geist, 2013a). For reasons such as this, understanding ways in which data is transmitted through networks is crucial for debating government and corporate policy that concerns digital life.

As discussed by Clement and Obar, Snowden has shown that the NSA intercepts internet data from all over the world while it transits through major US cities through splitter operations that copy and store the information (2014). In the tech world, this movement of data across national boundaries is referred to as "boomerang routing" and makes Canadian internet users vulnerable to NSA surveillance, even when both parties are communicating from within Canada in close proximity (Clement & Obar, 2014). As shown in one internal NSA PowerPoint slide from the Snowden documents, data packets of information move through fibre-optic cables through the cheapest route before reaching their final destination. As a result, much of Canadian data goes through the United States where it is intercepted and stored, before being bounced back to its final destination in Canada (Lyon, 2015; Clement & Obar, 2014). While investigating the paths of thousands of Canadian data routes, Geist and Wark found that almost 25% of Canadian data flowed through the United States before coming back to Canada, each time passing through cities with NSA splitters (2014). Because of the ways in which data flows across borders, national laws concerning data collection are easily evaded. This poses a threat to digital privacy rights:

> Once the data flows beyond the border, it no longer enjoys Canadian constitutional and other legal safeguards. This means the NSA or other US agencies can legally intercept and analyze it without warrants or other judicial oversight. Furthermore, Canadians have no legal basis to challenge or remedy any abuses (Clement & Obar, 2014: 27).

What is at play here is a larger force that extends beyond the legal rights of citizens of any given nation. In their book *Empire*, Hardt and Negri have commented on these forms of globalized power and the significance of mass surveillance within them. They argue that the globalization of surveillance is crucial for the functionality of contemporary forms of imperialism to flourish (2000). Thinking deeper about the role of government and corporate actors in 21st century politics, contemporary politics distort the boundaries of transnational corporations in collaboration with state efforts of control: "The concept of Empire is characterized fundamentally by a lack of boundaries: Empire's rule has no limits. First and foremost, then, the concept of Empire posits a regime that effectively encompasses the spatial totality, or really that rules over the entire 'civilized' world" (Hardt & Negri, 2000: xiv). Later, in *Commonwealth*, Hardt and Negri continue by asserting that biopolitical control (or governance over bodies and minds) relies on surveillance practices in order for authorities to maintain a dominant role in order to "primarily divide and segment the common field of productive cooperation" (Hardt & Negri, 2009:144), thus discouraging political organization and action against capitalism.

Likewise, Christian Fuchs notes that digital risks of exploitation and privacy invasion come not only from state governance but from corporate power (2014). Fuchs points to capitalism as a form of domination and control and a force that contradicts democratic freedom. Using the harsh state sanctions on whistleblowers in the United States as an example, he characterizes capitalism as a system in which alternative media cannot flourish or effectively disseminate information: "The economic, political, and ideological repressions that WikiLeaks faces are characteristic of the fact that the freedom of the media and information does not and cannot exist in capitalism" (Fuchs in Fuchs 2014: 11). For Fuchs, the resistance alternative media outlets face is one reason why political movements should aim to disarm structural power imbalances: "progressive

struggles have to be directed against capitalism and power asymmetries" (2014:11). More generally, he offers privacy law reform as a solution to one form of corporate exploitation: "given the right kind of government, states can also pass legislation that protects consumers' and employees' privacy from surveillance that serves corporate interests" (Fuchs, 2014:13). Fuchs supports Edward Snowden's actions as part of a larger movement of organizations and actors working to critique the commodification and surveillance-enabled structure of the internet:

> The actual practices of data commodification, corporate media control and corporate and state surveillance limit the liberal freedoms of thought, opinion, expression, assembly and association. These movements and groups are the negative dialectic of the enlightenment of the 21-st century informational capitalism. They show the difference between the proclaimed essence and the actual existence of liberalism (Fuchs, 2014:11).

As Fuchs enunciates this critique of liberalism, he believes more effort is needed in this direction, calling for a "society of equals, a participatory democracy" (Fuchs, 2015:11) as a solution to repressive state and corporate control over both the internet and society at large. As many discussions surrounding mass surveillance and civil liberties in the digital age touch upon the dynamics of corporate and government power, this has recently inspired some academics to rethink the exploitation of internet user activity through a Marxian analytic framework (Andrejevic, 2014). Fuchs differentiates between political and economic surveillance, noting that each operate by placing citizens under the threat of violence, albeit in different forms: "In the case of political surveillance, individuals are threatened by the potential exercise of organized violence (of the law) if they behave in certain ways that are undesired, but watched by political actors (such as secret services or the police)" (2013:7). In describing economic surveillance, Fuchs writes: "individuals are threatened by the violence of the market that wants to force them to buy or produce certain commodities and helps reproduce capitalist relations by gathering and using information on their economic behaviour. Violence and heteronomy are the *ultimo ratio*" (Fuchs, 2013: 7). For

Fuchs, both economic and political surveillance are about securing behavioural control of the masses by any means necessary, including the threat of violence in various forms.

While Fuchs recognizes that Marx's analysis of capitalist society alone cannot account for all the complexities of the modern surveillance state, his writing illuminates the significance of Marx's work for theorizing this type of research. Fuchs exposes the main goal of these combined activities as a means of maximizing surplus value through the exploitation of the labour force: "capital employs surveillance to control and discipline the workforce. Economic surveillance helps minimize the risk of making losses and maximizes the opportunities for profits" (Fuchs, 2013:9). He explains further by pointing to various ways in which surveillance works under the cycle of capital accumulation. To name a few examples, surveillance works to enhance capitalist relations through targeting future employees for background checks, using electronic or human supervision to evaluate workplace performance and protect private property, or following the data trails of consumers or market competitors (Fuchs, 2013: 8). Fuchs argues that the general logic of capitalist accumulation can be applied to support population management and control under capital:

> Marx's notion of accumulation as a central process of contemporary society plays an important role in unifying different approaches because modern society is based on the competition between actors accumulating ever more money capital, political power and ideological power and controlling the resulting resources. Marx is therefore not only important as a critical theorist of capitalism, but also in a more general sense, because he has pointed out a general law of movement in modern society originating in the capitalist economy that shapes all subsystems so that relatively autonomous subsystems have emerged based on the logic of accumulation. That is, modern surveillance is a competitive and instrumental process oriented towards accumulating money, power and hegemony (Fuchs, 2013:3).

While understanding surveillance as a core aspect of capitalism, Marx and Engels have elaborated on how the state monitors the population in various ways to maintain its power: "[The State] enmeshes, controls, regulates, superintends, and tutor's civil society from its most

comprehensive manifestations of life down to its most insignificant stirrings" (Marx & Engels, 1968:123 in Fuchs 2013). As characterized by Ogura (2006), the five forms of capitalist surveillance deal with population management, workplace surveillance, consumer behavior, control of the human mind, and digitalized surveillance (Ogura 2006 in Fuchs, 2013). Again, each form is concerned with monitoring and collecting information on bodies and minds in order to influence, predict, control or dissuade behaviour under capitalism, making it very difficult for individuals to discuss alternative politics or potential activist projects privately.

Following Manuel Castells' theory of informational capitalism, whereby technological advancements facilitated the switch from material labour to immaterial labour and resulted in the restructuring of western capitalism from the 1980's onward[1] (2009), Shoshana Zuboff has used the logic of accumulation to explain the undercurrents of modern surveillance under capitalism. "Surveillance capitalism" is a new form of capitalizing on the activity of others whose main purpose is to ultimately predict and manipulate consumer behaviour for profit" (Zuboff, 2015:75). Using the motivation of capital accumulation to collect as much data on internet users as possible, information on people's every move can be digitized, commodified, and sold to third-parties (Zuboff, 2016). Here, Zuboff's three laws of surveillance capitalism are also of relevance to explain the expansion of the surveillance state alongside the recent progress of the digital age:

> First, that everything that can be automated will be automated. Second, that everything that can be informated will be informated… [and third, in] the absence of countervailing restrictions and sanctions, every digital application that can be used for surveillance and control will be used for surveillance and control, irrespective of its originating intention (2013).

Mark Andrejevic also expresses the need for a critique of political economy to explain the intersection between surveillance and capitalism, as privacy-based arguments alone are inadequate

to explain the full level of exploitation at play: “privacy-based critiques do not quite capture the element of productive power and control at work in the promise of monitoring-based marketing… the critique of exploitation addresses this element of power and control" (2012:86). He also challenges readers to think about the future of society in the context of extensive digital surveillance methods that effect hundreds of millions of internet users:

> It is time to move beyond the question of whether or not we want targeted advertising- the real issue is whether or not we want to create a world in which every detail of our behaviour and communications with one another feeds into giant databases that are used to sort and evaluate us in ways that remain totally opaque to us, by a range of institutions whose imperatives are not necessarily our own (Andrejevic, 2013:189).

While various scholars have pointed out the ways in which internet users give up rights to their personal data in exchange for the use of so-called free services (Trottier, 2012; Schneier, 2015; Zuboff, 2015), Fuchs (2016) and Andrejevic (2013) have both drawn parallels between Marx’s alienation of labour and alienation involved in social media activity. Although the alienation of labour has traditionally underlined the exploitative experience of wage-labourers (Marx, 1844), this theory can be loosely applied to social relations of the digital era in that internet users lose ownership and control over their own online activity, which alienates them from this activity and its products. That is, they often have no knowledge of where their data goes, or for what purposes it is used thereafter. User-created content is handed over as a new form of free raw material (data) to big businesses who then use it to create new value through sorting, analyzing, and selling this data. At the same time, the same users who created it go uncompensated for their activity (Fuchs, 2016, Andrejevic 2013). Platforms such as Facebook and Google collect user data to provide a more intuitive browsing experience, which is reflected in the algorithmic sorting of data that ensures the most relevant information appears first. They also sell this data, such as demographic information, (sexual orientation, religious affiliation, age, income levels, behaviour patterns,

location data, friend lists, shopping habits, etc.) for profit, as third-party companies pay large sums of money for this information. As pointed out by cybersecurity expert Bruce Schneier, “Location data is so valuable that cell phone companies are now selling it to data brokers, who in turn resell it to anyone willing to pay for it” (2015:8), and these sales are taking place unbeknownst to users who are being tracked by GPS technology for these purposes. Outside of programs like AdBlock, internet users also have very limited options of the types of targeted advertisements they are subjected to, which puts their online experiences out of their control at yet another level (Fuchs, 2016).

In this form of exploitation, third-parties use this data for analytics and marketing purposes meant to predict, manage and control consumer behaviour. In the words of Zwick, Bonsu and Darmody, social media platforms rely on user generated data to "expropriate the cultural labour of the masses and turn it into monetary value: each in their own specific way but all according to the same general logic" (Zwick, Bonsu & Darmody in Andrejevic, 2012:72). Here, Andrejevic asks us to recognize “the importance of considering the components of exploitation (the capture of unpaid surplus labour, coercion, and alienation) [that] operate within the context of technologically facilitated forms of commercial surveillance” (2012:87). The concept of alienation as applied to digital age online participation effectively demonstrates another way in which Marx remains relevant for critiquing 21st century surveillance tactics.

Moving forward, reference to Foucault’s ground-breaking work on early forms of surveillance and disciplinary society (1977) is helpful. Of equal relevance to the contemporary context of state power exercised as surveillance is Deleuze’s subsequent commentary on societies of control (1992). Deleuze weighs in on new forms of social sorting through technology, as

individuals are reduced to their data bodies, which Deleuze refers to as ‘dividuals’, entities to be managed and monitored by companies and law enforcement agencies: “The numerical language of control is made of codes that mark access to information, or reject it. We no longer find ourselves dealing with the mass/individual pair. Individuals have become *‘dividuals,’* and masses, samples, data, markets, or *‘banks’"* (Deleuze, 1992:5). As defined by Williams, a "dividual” refers to “a physically embodied human subject that is endlessly divisible and reducible to data representations via the modern technologies of control, like computer-based systems” (2005:2). Because liquid surveillance (Lyon 2015) has extended far beyond the confines of the institution, it is often argued that the panoptic threat that ultimately controlled bodies within prisons, schools or places of work has transcended that old model. In this view, we have moved away from Bentham’s vision of the panopticon as presented by Foucault (1977), whereby the very possibility of always being visible within institutions forces people to alter their behaviour (Foucault, 1977:200). Through technological means, new age surveillance has seeped into digital devices, exposing our innermost private thoughts, relationships, plans, and conversations. For this reason, according to Simon (2005), this new electronic realm does not signify the death of Bentham’s panopticon, but has only expanded it. Under the reign of “new surveillance” or “dataveillance”, the population is under even harsher scrutiny than previously imagined: “What makes databased selves different from our actual selves is that databased selves are more easily accessible, observable, manageable and predictable than we are. Databased selves actually meet the Benthamite ideal better than the disciplined bodies of the Panopticon” (Simon, 2005:16). In this day and age, the very possibility of being watched at any given time has become a fathomable reality, even within the confines of our own homes.

On the topic of data bodies and data trails, Snowden advocates for the important possibility to remain anonymous online, as the fear of being surveilled breeds self-censorship and hinders education. In CITIZENFOUR, a documentary about his meeting with reporters in Hong Kong to discuss and hand over the leaked NSA documents, Snowden asserts that the very knowledge of being potentially surveilled online "curtails intellectual freedom" and "limits the boundaries of intellectual exploration" where people are afraid to write or research on certain topics out of fear of ending up on a government watch list (Poitras, 2014:26:55-27:20). We can interpret this fear using Foucault's concept of governmentality, whereby entire populations are socialized to conform and govern their own actions and thinking through various institutional and cultural norms alongside the implicit threat of fear-based policing (2007). The existence of mass surveillance can be harmful to social movements and political progress; in Greenwald's words: "history shows that the mere existence of a mass surveillance apparatus, regardless of how it is used, is in itself sufficient to stifle dissent. A citizenry that is aware of always being watched quickly becomes a compliant and fearful one" (2014:3). In this case, governmentality describes the situation when users avoid using the internet in certain ways, self-policing their own internet research and social connection due to fear of being targeted for extra surveillance. Pew Research has indeed shown that at least 34% of Americans have made some attempt to privatize or change their internet habits since learning of the Snowden revelations (Rainie & Madden, 2015).

Next, the subject of whistleblower protection is an important aspect within literature on the Snowden files. While media controversy surrounding whistleblower Chelsea Manning's harsh prison sentence is ongoing (Pilkington, 2015), there has been much subsequent debate about what to do with Edward Snowden. As discussed in "Protecting News in the Era of Disruptive Sources" (Wasserman, 2015), members of the press enjoy certain immunities to legal scrutiny that

whistleblowers do not. Even though the press needs whistleblowers for serious investigations of questionable government and corporate practices, media organizations often do little to help their sources in terms of legal protection (Wasserman, 2015). Wasserman, a professor of journalism and ethics at Washington and Lee University, argues that the Snowden case can serve as either a deterrent or inspiration for future whistleblowers, depending on how the US handles his capture or release. Snowden has been charged under the Espionage Act[2] but due to the valuable information Snowden revealed, Wasserman argues that Snowden should be entitled to a fair trial with a strong legal defense, which is currently not an option. For Wasserman, Snowden's charges should reflect the significance of his disclosures: "something appropriate to the enormity of the wrong-doing he has exposed, something that helps make the country safe for others who have stories the public is entitled to hear" (2015: 118).

Here, the legal protection of whistleblowers is important to the larger issues of freedom of speech, government transparency, and future of democratic information networks. Wasserman explains that the digital revolution of communications can either result in unprecedented emancipation or suppression. As we have seen with recent "fake news" scandals following the Trump election, technology alone does not guarantee the sharing of true or high quality information, nor does it guarantee meaningful public dialogue. Wasserman argues that political journalism and whistleblowing can only flourish if sources can enjoy proper protection and fair legal processes:

> People who have information [of public significance] believe it will be heard and welcomed, and if they can step forward with it without fear of punishment. That's why the whole edifice of informational freedom in the digital age depends on creating and environment in which sources can speak (Wasserman, 2015: 119).

Traditionally, because of the thick veil of secrecy safeguarding the secrets of intelligence agencies, whistleblowing has been the only catalyst for reform in the intelligence community (Cullather, 2015:23; Hamilton, 2014). Bruce Schneier (2015) and Glenn Greenwald (2014) have both shared similar sentiments, stating that whistleblowers and journalists need better legal protection to expose serious wrong-doing. Schneier suggests that government whistleblowers should benefit from the same legal protections that corporate whistleblowers enjoy. This does not suggest that anyone should be able to leak any information and call themselves a whistleblower. The argument is that there should be appropriate legal framework and protocol for leaking sensitive information, by which courts could evaluate leakers on a case by case basis, where the defendants have a chance to defend their actions from a moral standpoint in front of a jury of their peers (Schneier, 2015).

While whistleblower protections are weak, so too are the rights of internet users in general, especially when dealing with governing bodies outside of their own countries. As state and corporate actors work together to maintain control of the internet and its users, Tim Berners Lee, the creator of the World Wide Web, has been calling for a public collaboration on "A Magna Carta for the Web", as the corporatized internet in its current form is uncoordinated with its true democratic potential of information sharing and non-hierarchical power structures (2014). As stated by Schneier, this effort would "restrict the actions of both governments and corporations, and impose responsibilities on information-age corporations rather than just rights" (2015: 149). Along these lines, work from the Berkman Center for Internet and Society at Harvard University investigates thirty different web advocacy initiatives working towards an "Internet Bill of Rights" or "digital constitutionalism" between 1999-2015. The authors use this term to categorize a variety of efforts working towards "political rights, governance norms, and limitations on the exercise of

power on the internet" that have the potential to change governmental and corporate policies concerning internet use (Gill et al., 2015:2). Gill, Redeker and Gasser map the trajectory of influential organizations, hacktivists, cryptographers, journalists and others that have been taking action towards making the internet a decentralized, democratic space for free speech, anonymity and information sharing (Gill et. al, 2015). In hopes of pushing public policy and law in the direction of digital constitutionalism, the authors explain how the Snowden documents have positively influenced discourse on privacy rights initiatives:

> In particular, we see marked overall increases in the occurrence of the right to data control and self-determination, the right to anonymity, the right to use encryption, and the right to explicit protection from government surveillance. Our hypothesis, borne out at least in a preliminary way by this data, is that while the perceived importance of privacy rights was not substantially affected, they are now being articulated in much more specific, sophisticated, and nuanced ways than they have been in the past (Gill *et al.*, 2015:17).

Despite the wide range of differences between initiatives to democratize the internet, these efforts are grouped together based on this common goal "and are usefully understood as part of a broader proto-constitutional discourse" (Gill et al., 2015: 2). Activist initiatives to protect the legal use of strong encryption are also of relevance here, as the political and legal landscape is still unfolding in terms of questions of who governs the internet as well as what constitutes legal online activity. Additionally, this article demonstrates the significance of discourse, activism, and academic investigation on digital rights by making reference to the International Principles on the Application of Human Rights, stating that Snowden's documents have only expedited the significance of these movements: "[n]othing could demonstrate the urgency of this situation more than the recent revelations confirming the mass surveillance of innocent individuals around the world" (Gill et al., 2015:17)[3].

As the internet has been exposed to be a risky place for private communication due to pervasive surveillance on multiple levels, the concept of risk itself is worth exploring. Social theorist Ulrich Beck has also commented on Big Data surveillance in lieu of Snowden by expanding on his 1992 theory of risk society. In 2013, he coined the term "Global Digital Freedom Risk" to refer to the heightened risks involved for internet users in the 21st century, where activist groups are heavily targeted as blanket surveillance operations become normative. Beck calls for a "digital humanism" when he writes: "Let us identify the fundamental right of data protection and digital freedom as a global human right, which must prevail like any other human right, if needs be against all odds" (2013)[4]. Following Beck, digital sociologist and risk studies scholar Deborah Lupton identifies three components of "Digital Risk Society" in a paper with the same title. As activism has become increasingly criminalized with harsher sentences, digital activists also take on the risk of violence perpetuated by the state. More generally, mass surveillance makes private digital communications risky, as users lose track of their own digital movements. In terms of the digital divide, those without internet access face different types of risks in this new age concerning opportunities and life chances (Lupton, 2014). Lupton calls for traditional risk studies to move towards digital sociology and surveillance studies to create a more comprehensive inter-disciplinary understanding of how to grapple with the struggle of the increasingly pervasive risks associated with communications technology (2014).

Published a year before the first Snowden disclosures, Daniel Trottier's book *Social Media as Surveillance: Rethinking Visibility in a Converging World* investigates the risks of using social media by studying Facebook as a new social dwelling (2012). Trottier explores the ways in which users live and interact online as well as who is watching their behaviour. Facebook, once an exclusive platform for university students to communicate with each other, has turned into a

massive network early users no longer recognize. Over the past decade, as parents, grandparents and work colleagues have joined the site, the overall structure and social significance of the dwelling has drastically changed. Thus, users are not only being watched by their own network of "friends" but also their employers (present or future), their universities, the police, government agencies, third-party corporations, and of course, Facebook itself. Most significantly, local law enforcement agencies have gained access to backchannels of social media quite some time ago, and new additions to the platform such as facial recognition have made evidence collection on social media easier for police departments (Trottier, 2012).

Trottier uses the aftermath surrounding the Vancouver Hockey Riots as an example of crowd-sourced surveillance on Facebook, where thousands of people shared images and videos of the riots while others identified them to help police catch rioters on designated Facebook groups. While Trottier appreciates the many benefits of new communication technologies, he also explores surveillance as "the driving force behind social sorting, the allocation of life chances and business models in the information economy" (2012:7). For Trottier, one of the biggest risks of greater public visibility on social media is giving law enforcement unprecedented access to information it otherwise had no means of legally attaining. As social media sites become dwellings for larger segments of the general population, the convergence of government, corporate, activist, criminal and social interests find a new site of intersection, marking the internet an emerging social space for sociological inquiry (Trottier, 2012).

As mentioned above, Zuboff theorizes on how technology helps to enhance the mass surveillance project, and will continue to do so unless meaningful oversight or limitations of power are imposed on it. As a result of new technological capabilities and a lack of legal regulations to

keep up with them, companies who engage in data collection have far more power over their clients than those who do not. In one example, Zuboff points to insurance companies who follow Google's business model of data mining to collect and sell information on their clients to increase profit. Car insurance companies are beginning to use GPS technology to collect data on driving habits, which can result in higher insurance rates, time-stamped location data and the possibility of shutting engines down remotely as a response to late payments or aggressive driving (2015). Zuboff's article "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization" (2015), investigates Google as a key perpetrator of surveillance capitalism as the king of Big Data analytics. As the world's most visited website, Google has been the leader in Big Data analytics, paving the way for Facebook and other notable internet firms to collect and store mass amounts data to sell to advertisers (Zuboff, 2015). Google puts innovation before everything else including the legality of its own actions. Zuboff uses the example of Google's Street View project where Google took the liberty of taking photos of homes across the globe without obtaining any sort of permission, illegally scraping their personal Wi-Fi data along the way (Zuboff, 2015). Google has taken advantage of a time where both the law and user understanding are perpetually a few steps behind new communications technology. Consequently, once privacy laws are set in place to secure user data, companies like Google will use the same arguments for privacy rights to hide its own activity:

> Surveillance capitalists have skillfully exploited a lag in social evolution as the rapid development of their abilities to surveil for profit outrun public understanding and the eventual development of law and regulation that it produces. In result, privacy rights, once accumulated and asserted, can then be invoked as legitimation for maintaining the obscurity of surveillance operations (Zuboff, 2015: 83).

By extension, the business models and unprecedented data accumulation of these companies are what makes today's extensive state surveillance possible in the first place. Zuboff

challenges Google's Chief Economist, Hal Varian, in his view that predictive analytics will make new social contracts possible in a progressive way, where the Google users will "voluntarily" give up even more of their behavioural data in exchange for high tech services such as digitalized personal assistants that know what you want even before you do. Instead, Zuboff argues that a constantly surveyed reality will result in the end of social contracts and the absence of consumer choice: "In Varian's economy, authority is supplanted by technique, what I have called the 'material dimension of power' in which impersonal systems of discipline and control produce certain knowledge of human behaviour independent of consent" (Zuboff 2015:81). As the White House and Google both fully intend to continue mining as much internet data as possible, Zuboff warns predictive analytics are harmful to the concept of the democratic right to privacy. The way data mining is currently performed under Castells' "information capitalism" (2009) perpetuates power imbalances and damages life changes by "predict[ing] and modify[ing] human behaviour" for the sake of profit (Zuboff, 2015: 75). Under surveillance capitalism, the relationships between producer and consumer or capitalist and labourer have changed. First, Google's customers aren't its users, but their advertisers (Zuboff, 2015). Second, though Google employs tens of thousands of people, its most valuable material (data) is collected for free, from users who (however unknowingly) provide massive amounts of personal data to be analyzed and sold to third-parties daily. In a 2009 *Wired* article, Varian explains that Google offers its services for free because user action holds value for corporations, and more web traffic inevitably leads to more ad sales: "since prediction and analysis are so crucial to AdWords, every bit of data, no matter how seemingly trivial, has potential value' (Levy, 2009 in Zuboff, 2015:79). This, combined with smart technology and wearables, creates a reality where every single human movement is potentially commodifiable by outside forces. Outlining the threat to freedom and social contracts that this type

of surveillance culture implies, Zuboff critiques Varian's optimistic view of the future of behavioural data mining. Google's ideology does away with the very possibility of privacy as a choice at all. When the inherent trust is taken out of traditional contracts between buyer and seller to be replaced with digital surveillance that renders all human activity 'certain', Zuboff argues: "deception-induced ignorance is no social contract, and freedom from uncertainty is no freedom" (2015:86).

Data mining projects will only get more sophisticated and deeper in breadth. To highlight this point, Zuboff quotes a 2014 White House report: "The technological trajectory, however, is clear: more and more data will be generated about individuals and will persist under the control of others" (White House, 2014: 9 in Zuboff 2015: 75). The future plans of internet giants only seek to expand data mining capabilities alongside their own profitability, capturing anything they can about users' immediate reality. We see this happening with the rise of "smart" technology, wearable sensors and GPS technology used to share private health data, and patterns of movement to surveillance databases (Zuboff, 2015). Predictive analytics are the next step towards influencing and controlling consumer activity, as insurance rates (Zuboff, 2015), employment opportunities (Schneier, 2015), and bank loans (McCrum, 2015) are becoming increasingly dependent on digital data collection. Schneier likens this level of surveillance to extending the way celebrities and politicians are constantly scrutinized to the general population (2015). Internet users are penalized in ways they may not even be aware of by their own data content. In defense of the NSA after the initial Snowden leaks reached the public, Robert Litt, General Council for the Office of the Director of National Intelligence explained the NSA's intentions to make use of new technologies to fight crime: "Rather than attempting to solve crimes that have happened already, we are trying to find out what is going to happen before it happens" (Fidler, 2015: 104).

From a critical standpoint, one way predictive analytics are ethically problematic is due to the threat of digitalizing the same racist and classist bias already embedded within some traditional law enforcement practices in the United States and elsewhere. History has shown that regardless of the method, marginalized populations and dissidents are consistently surveyed the most (Greenwald, 2014; Hamilton, 2014; Lynch, 2012). Just as new biometric technologies often discriminate against disabled bodies or people of colour (Magnet, 2011), algorithmic crime-prediction programs may have racial discrimination built into their systems as well, targeting areas which are already heavily policed to begin with, which are most often communities of color in the United States (Eubanks, 2014; Lynch, 2012). Hewitt argues that while discriminatory targeting is not new, the possibilities of reach have greatly expanded: "certain groups and individuals have long been subjected to more intrusive surveillance, and dramatic consequences as a result of that attention, because of their ideology, race, ethnicity, gender, sexuality, religion, nationality, social class, or some combination of these variables" (Hewitt, 2015:46). The potential outcomes of this type of information access by third parties can be life changing for the individuals involved. As users lose control over their private identities online, information meant to be shared with close friends may be accessed by future employers, family members, the police or national intelligence. The intimate details of sexual preferences, religious affiliations and medical history are made available to various entities without consent or knowledge (Schneier, 2015). To circumvent this from happening, strong legal protection against the abuse of mass surveillance programs is needed. As aptly concluded in Zuboff's analysis: "The question is whether the lag in social evolution can be remedied before the full consequences of the surveillance project take hold" (Zuboff, 2015:85).

## Methods

This research uses a mixed methods approach to examine the current state of internet surveillance as well as activist initiatives against them. To quote David Lyon, surveillance embodies "processes in which special note is taken of certain human behaviours that go well beyond idle curiosity" (Lyon, 2007:13 in Trottier, 2012:7). Here, activism against mass surveillance can include anything from government whistleblowing, to alternative open source software development, to teaching internet users to secure their digital communications and activity, to mobilizing people to sign petitions protesting against controversial legislation. Because the Snowden story is still unfolding at the time of this writing, this thesis has been informed by a mix of qualitative interview data, recent online video footage of Snowden at events and conferences, Snowden's commentary on social media platforms such as Twitter and Reddit, news media publications about the ongoing disclosures, and by relevant academic literature on the topic of the contemporary surveillance.

To better understand the state of US and Canadian policy in regards to digital surveillance practices and law, four semi-structured interviews were conducted with activists and academics working on relevant projects in the Montreal area. These interviews were primarily conducted in the early stages of this project to aid my comprehension as an emerging scholar with little to no background knowledge in the field of law and technology. After obtaining the appropriate ethics approval from Concordia University, the following people were interviewed and have each graciously agreed to have their identities published for this project:

(1) Dmitri Vitaliev: founder and director of Equalitie, an expert on technology training who has been working on digital privacy initiatives in over 40 countries over the last 10 years. His

organization develops open-sourced software and protects client websites from malicious attacks[5] and hosts free techno-activism events every third Monday to better educate the Montreal community about digital security.

(2) Evan Light: post doctorate fellow at Concordia University's Mobile Media lab who has created a mobile offline version of the Snowden Archive to make the documents accessible to researchers and journalists without being monitored. As part of Light's research, he presents information about the Snowden documents at conferences across the globe.

(3) Arron Thaler: McGill engineering major and founder of Montreal-based activist organization against bill C51: The Student Coalition for Privacy[6]. Thaler has also worked for Privacy International and the American Civil Liberties Union and has helped build a legal case against the GCHQ using the Snowden documents as evidence.

(4) Lex Gill: McGill law student who has recently worked with the Berkman Center for Internet and Society at Harvard as well as the Canadian Civil Liberties Association. She is also a former Google Policy Fellow at the Canadian Internet Policy and Public Interest Clinic. Gill's ability to educate others on the democratic importance of privacy has inspired this project at large. Her passion and willingness to share her extensive knowledge about the technical and legal mechanisms of the surveillance state has profoundly contributed to my own perspective on this topic.

In addition to interview data, this research relies on select Snowden documents pertaining to civilian surveillance programs within the US and Canada. Because the original documents are highly technical, laden with insider lingo and abbreviations, journalistic articles that interpret the

documents from news publications such as *The Guardian*, *The Intercept*, and *The Washington Post* are largely referenced throughout this thesis. The reason for using these particular news sources is because their own journalists were carefully selected by Snowden to distribute the NSA documents in the first place.

---

[1] According to Castells, informational capitalism "is linked to the expansion and rejuvenation of capitalism, as industrialism was linked to its constitution as a mode of production" (2000:19)

[2] See United States v. Snowden, 2013

[3] "International Principles on the Application of Human Rights to Communications Surveillance," Necessary and Proportionate, last modified May 2014, https://en.necessaryandproportionate.org/text. From (Gill et al., 2015)

[4] https://www.opendemocracy.net/can-europe-make-it/ulrich-beck/digital-freedom-risk-too-fragile-acknowledgment

[5] See https://equalit.ie/ for more information

[6] See Student Privacy Coalition https://studentprivacy.ca/

## Chapter Two

## The Robin Hood of the Information Age

*"I used to work for the government. Now I work for the public"*

– Edward Snowden (Twitter, 2016)

Before being exiled to Russia, his life thrown into a whirl-wind of legal charges and media controversy, Edward Snowden led a simpler life. Working as a 29-year-old contractor for the National Security Agency (NSA) with a promising career as an infrastructure analyst, Snowden was making an annual salary upwards of $100 000 from his work station in Hawaii (Booz Allen Hamilton, 2013). Then, in the spring of 2013, he made a life-changing decision to make copies of tens of thousands of classified NSA documents and flee to Hong Kong to share them with carefully selected journalists. While Snowden never intended to live in Russia, he has been trapped there since the US government cancelled his passport in transit from Hong Kong to South America. According to Sarah Harrison, the WikiLeaks editor who had helped Snowden travel from China to Russia, he refused a job offer from Russian intelligence upon his arrival to the Moscow airport. Russian authorities kept him in the airport terminal for 21 days before deciding to let him in to the country where he has been living under temporary asylum since 2013 (Goetz & Heilbuth, 2015).

With a great understanding of the inner workings of digital communications technologies and an even stronger moral compass, Snowden had pointed out the questionable legality of civilian spy programs to his supervisors, but to no avail. Respectively, his self-proclaimed love for his country is what has propelled him to engage in what the BBC has championed the "biggest leak of top-secret intelligence documents the world has ever seen" (Taylor, 2015). The documents in question contained information pertaining to the ways in which the Five Eyes (governments of the US, Canada, Australia, the U.K and New Zealand) engage in civilian spy programs, secretly

collecting the personal information of hundreds of millions of people. Since 2003, government data collection on civilians has included the contents of e-mails, chats, texts, phone calls, location data, online purchases, search history, and shockingly, even pornography-watching habits, personal webcam images and videos, including those of the explicit variety (Ackerman & Ball, 2014). These programs are not being used exclusively to collect information on targeted suspects of crime or terrorism, but for the bulk collection of data on all AT&T or Verizon Wireless cellphone users and anyone using Google, Facebook, Yahoo, Microsoft, Apple or Skype (Greenwald, 2014; Schneier, 2015; Mills, 2015).

Knowing he would be charged with serious criminal allegations at the federal level for sharing these documents (Poitras, 2014), Snowden explains that he went to the press because he believed the public has the right to know about government spy programs which secretely spy on their own populations on an untargeted basis (Poitras, 2013). In an printed interview with the public hosted by *The Guardian*, Snowden explained his motivation:

> It was seeing a continuing litany of lies from senior officials to Congress - and therefore the American people - and the realization that that Congress, specifically the Gang of Eight, wholly supported the lies that compelled me to act. Seeing someone in the position of James Clapper - the Director of National Intelligence – boldly lying to the public without repercussion is the evidence of a subverted democracy. The consent of the governed is not consent if it is not informed (Snowden, 2013).

Though all three branches of government may have approved the NSA programs, they were performed under a thick veil of secrecy and hidden from the public eye. Snowden understood the unwarranted mass collection and storage of personal data to be unconstitutional under the 4th amendment. Indeed, protection against unreasonable search and seizure by the state are rights granted to American citizens under the Constitution. In Canada, Section 8 of the Charter of Canadian Rights and Freedoms[1] also safeguards citizens against unreasonable search and seizures,

but Canada is still heavily involved with the mass surveillance activities of the Five Eyes. Under the Harper government, Canada has recently pushed to give the Canadian Security Intelligence Service (CSIS) even greater surveillance and policing powers under Bill C51 in 2015.

As will be explored later in Chapter Three, intelligence agencies play by their own rules, answering only to their own internal review boards or secret courts who use their own interpretations of secret laws which are not available to the public (Schneier, 2015). Florida Congressman Alan Grayson has gone as far as to say that "NSA congressional oversight is a joke" (Grayson, 2013). As our legal systems struggle to keep up with new technological innovation and the culture of digital communication while intelligence agencies get carte blanche from secret courts such as the Foreign Intelligence Surveillance Court (FISC), digital rights remain unstable and largely unchartered. Snowden argues that our digital property and communications should fall under the same legal rights as any other property and communications and should not be subject to warrantless surveillance by secretive government initiatives (Pilkington, 2015a).

But who exactly is Edward Snowden and why should the public trust him? Despite media attention on his personal life, he has repeatedly maintained that it should not matter who he is, as he has tried to curtail public interest in his personality. In an interview with *Wired,* Snowden has asked the public to ignore their feelings about his personal character: "If I'm the worst person in the world you can hate me and move on…What really matters is the kind of internet we want, the kind of relationship with society... I wouldn't use words like hero or traitor. I'm an American and a citizen" (Rowan, 2014). Snowden has done a good job at managing his own public relations, making frequent appearances at video conferences and engaging in political discussions at academic institutions around the world. Highly articulate and well-versed in speaking to both the

technical and legal aspects of his arguments, he takes the moral high ground, frequently referencing the US Constitution and the upmost importance of protecting civil rights.

Of course, not everyone agrees with Snowden's politics. In the summer of 2013, NSA representatives were quick to discredit Snowden's information by pegging him as a "narcissistic fame-seeker", even though, as pointed out by Glenn Greenwald in a joint-interview with Noam Chomsky, Snowden did not appear on one mainstream news program despite a year of the phone ringing off the hook with journalists begging for an interview (Greenwald, 2014). Meanwhile, Pew Research has shown that the public remains split in their support of his decision to leak classified documents, age serving as a variable in whether Americans view Snowden as a criminal or a hero: "57% of 18- to 29-year olds said the leaks have *served* rather than harmed the public interest — almost exact mirrors of the 65-and-over age group" (Desilver, 2014:1)[2]. In the words of NSA director Michael Hayden during a televised interview, Snowden's actions were "arrogant":

> It was the arrogance of an individual, who looked upon the activity of the National Security Agency and believed that it was his legal and ethical judgment that trumped the judgment of his co-workers, his leadership, the American president, the American Congress, and the American court system in order to create a moral rightfulness that he claims. That's pretty arrogant. (*Goetz & Heilbuth, 2014).*

Others are on the fence not about what he did, but how he did it, as is the case with former member of the House Select Intelligence Committee, Lee Hamilton. Hamilton argues that Snowden mishandled classified information, but the leaks themselves were warranted: "we are in a better position to ensure the future lawbreaking is not required to address the exercise of secret, expansive government power…the potential for someone to at some point to abuse that [government] power and turn it against the American people is worrisome" (Hamilton, 2016:48).

Reddit, an online space for information sharing and quasi-anonymous discourse, has been closely following the Snowden debate over the last few years. The popularity of Snowden's AMA sessions[3] (Ask Me Anything) as well as the frequently occurring front page discussions on Snowden generally indicate Reddit's interest in the leaks. A quick discourse analysis of a Reddit thread titled: "On the surface Reddit is very Pro-Snowden, but can anyone make a good argument to oppose the actions of Edward Snowden?" reveals the most frequently reoccurring arguments against him[4]. With over four thousand comments from Reddit users, people have argued that Snowden is a "traitor", guilty of treason, asserting that he had no right to release such important information that could potentially damage national security. Non-supporters also argue that even if Snowden was in the right, he has set a dangerous precedent for other security workers who feel self-righteous enough to leak the "wrong" secret documents to the public that could cause serious damage to national security. From the very first leak, following discourse from mainstream media outlets, public opinion has been split on the topic of Snowden as hero or traitor in the United States. In his defence, Snowden asks: "The question is, if I was a traitor, who did I betray? I gave all of my information to American journalists and free society generally" (AP, October 5, 2015). Interestingly, outside of the US, in other parts of the world such as Europe, people are less concerned with questions of Snowden's personal level of patriotism and more interested in the content of the leaks themselves (Snowden, 2016b).

Despite his circumstances, Snowden's sarcastic sense of humour shines through via his online presence and engagements. For example, in 2015, former NSA/CIA director Michael Hayden threatened Snowden's safety in a TV interview: "If you're asking me, my opinion, he's gonna die in Moscow, he is not coming home," (Bradburn, 2015)[5]. Shortly following that comment, Snowden posted a photo of himself with Hayden to his Twitter profile captioned:

"Disappointed that Michael Hayden is implying I'll be killed in Moscow. He used to be more fun"[6].


As Snowden remains in Moscow, he uses the internet as a window to the outside world. At least in digital form, he can be anywhere he needs to be around the globe (Heuvel & Cohen, 2014). In an interview with *The Nation*[7], Snowden explained that he has built his own studio and sets up secure live video chat sessions in the way that newscasters do. This has allowed him to participate at many conferences and interviews across the globe which are both livestreamed and recorded for public access online (Heuvel & Cohen, 2014). Perhaps the most impressive display of Snowden's unwavering ability to communicate with the outside world from exile was his appearance at TED2014. In a presentation titled "Here's How We Take Back the Internet", Snowden appeared as a telepresence robot in a thematically-appropriate display of technological-futurism. He controlled the robot remotely from Moscow, wheeling it around the Vancouver conference at will.

*Chris Anderson with Edward Snowden. Photo from Wired.com*

The massive scale of top-secret intelligence data that Edward Snowden had access to could have been shared in a variety of ways. It could have been sold to the highest bidder of competing governments or spies in other countries, or it could have been carelessly uploaded in bulk onto WikiLeaks which could have potentially led to national security risks in the United States or put NSA employees in danger. Instead, Snowden went a different route, one that was calculated carefully. As a network analyst, he understood that his role was not to decide what sensitive NSA documents should be made public, but to hand that responsibility over to a handful of journalists that he trusted, and he asked them only to publish documents that they thought would serve a public interest, none that would cause any harm (Snowden, 2016b). Investigative news media have

been put in place to protect the constitution by serving as a watchdog to the government since the early days of the United States, a system in which journalists play a key role in upholding democratic values such as freedom to information (Kovach & Rosenstiel, 2001). Because journalists have the legal protection of the First Amendment on their side, *The Guardian's* Glenn Greenwald and others have been able to share Snowden's now-famous classified NSA documents with the world without being charged (Greenwald, 2014a).

Under the Espionage Act, Snowden has been charged with "unauthorized communication of national defense information" and "willful communication of classified communications intelligence information to an unauthorized person," (United States v. Snowden, 2013) and faces up to thirty years in prison should he return to the US. The Obama government has been particularly harsh on whistleblowers compared to previous administrations (Schneier, 2015) and was quick to charge Snowden. Under his presidency, Obama has charged seven people under the Espionage Act which was originally put in place to deter US soldiers from aiding state enemies in times of war. Before Obama, only two other people had ever been charged under the Espionage Act since it was first passed in 1917 (Schneier, 2015). In Schneier's view, treating "journalism as a crime" in this context is "extraordinarily harmful to democracy", as "public disclosure in itself is not espionage" (Schneier, 2015: 128).

Notably, in 2013, 24-year old US army intelligence analyst Chelsea Manning was also convicted under the Espionage Act after sharing millions of Afghan War documents with WikiLeaks. She was sentenced to 35-years in military prison in the US (Pilkington, 2015b), and has been subjected to treatment that the UN special rapporteur on torture has described as "cruel, inhuman and degrading" (Pilkington, 2012). Understanding the potential legal outcomes of his

actions following Manning, Snowden has repeatedly affirmed that he would gladly return to the US for a fair trial to face a jury of his peers (Greenwald, 2015) and is allegedly still waiting for an offer from the US government to do so. As recounted in an article from CBS News and the Associated Press, “Snowden told the BBC that he'd volunteered to go to prison with the government many times,” (2015) but had not received a formal plea-deal offer. “So far they've said they won't torture me, which is a start, I think,” Snowden laughed, “But we haven't gotten much further than that" (CBS & AP, 2015). Under the Espionage Act, an opportunity for a fair trial is highly unlikely because Snowden would not be able to make a public interest defence or even use the word “whistleblower” during his testimony (Snowden, 2016). The harsh sentences used by the US government are a tactic to deter others from leaking sensitive information, such as in the Chelsea Manning case. Those charged under the Espionage Act are judged in private court proceedings by special judges and are typically not allowed to explain the motivations behind their actions as part of their legal defence strategy (Greenwald, 2015; Schneier, 2015; Trimm, 2013). As a result, Snowden has remained in Moscow for the last three years, appearing at conferences and university events via live video streaming.

Snowden’s disclosures have added a sense of urgency to a digital privacy debate that precedes him by a couple of decades. According to Zuboff, this topic is of robust political significance, causing authors of scholarly literature to address “many substantial concerns associated with the anti-democratic implications of the concentration of privacy rights among private and public surveillance actors” (Zuboff, 2015:83). The Snowden documents have provided substantial proof that the internet and cellphone technology have become instrumental to pervasive mass surveillance due to the corporatization of the web. Conversely, they have also served as tangible evidence in court cases against the NSA, such as in *ACLU v. Clapper* of 2015, where the

American Civil Liberties Union (ACLU) won a case against the NSA on appeal. Ultimately, the Supreme Court ruled that section 215 of the Patriot Act did not permit the bulk collection of cellphone metadata. The NSA had been collecting any data "relevant" to a terrorist investigation, arguing that since they did not yet know what was "relevant" they collected all telephone metadata. The Court ordered the termination of the program (Snowden, 2016B): "Whatever Section 215's 'relevance' requirement might have allowed; it did not permit the government to cast a seven-year dragnet sweeping up every phone call made or received by Americans. The court of appeals agreed" (American Civil Liberties Union, 2015).

Though it is too early to foresee the full social effects of the Snowden disclosures, at the time of this writing, his story stays relevant in media headlines and should be of equal interest to critical sociology. The popularity of the Snowden story is only expected to increase after Oliver Stone's feature film, *Snowden,* which made its debut in September 2016. At the risk of his own exile and possible imprisonment, Snowden's characterizes his own actions as resistance against state powers that extend beyond regulatory law and public consent (Snowden, 2016). In his efforts to share classified intelligence documents with the public, his main objective to spark a political discussion around the liberal democratic compatibility with mass surveillance has been realized. As Chapter Two has explained Snowden's perspective and his motivations for whistleblowing, Chapter Three explores the content of some of the classified documents that have been publicly shared by *The Guardian* and other media outlets.

---

[1] See Section 8 of the Canadian Charter
http://www.pch.gc.ca/eng/1356636395105/1356636488152#a8

[2] (Desilver, 2014) Most Young Americans Say Snowden has Served the Public Interest: http://www.pewresearch.org/fact-tank/2014/01/22/most-young-americans-say-snowden-has-served-the-public-interest/

[3] We are Edward Snowden, Laura Poitras and Glenn Greenwald, from the Oscar-winning documentary CITIZENFOUR. Ask Us Anything https://www.reddit.com/r/IAmA/comments/2wwdep/we_are_edward_snowden_laura_poitras_and_glenn/, and Just days left to kill mass surveillance under Section 215 of the Patriot Act . We are Edward Snowden and the ACLU's Jameel Jaffer, Ask Us Anything https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under

[4] Ask Reddit On the surface Reddit is very Pro-Snowden, but can anyone make a good argument to oppose the actions of Edward Snowden

[5] BBC interview with Hayden https://www.youtube.com/watch?v=lkwrQ6p9JAM)

[6] Link to Twitter post https://twitter.com/Snowden/status/651459385445720064

[7] Snowden interview with the Nation

# Chapter Three

## Civilian Spy Programs: Effectiveness, Exploitation, and Legality

Data collection and analytic tools are used for much more than showcasing tailored ads on the right-hand side of Facebook newsfeeds. Unsurprisingly, intelligence agencies and law enforcement have joined forces in using the data mining technologies spearheaded by corporations. The same data collected by internet service providers (ISPs), phone companies, social media platforms and associated third-parties, are further monitored by the intelligence agencies of the Five Eyes, who have been quietly collecting as much digital information as possible on both foreign and local populations since 9/11 (Greenwald, 2014; Schneier, 2015). When questioned about civilian spy programs, intelligence agencies of the US and Canada first denied the existence of these programs, and once exposed through Snowden's evidence, justified them by insisting that national security is at stake. One week after *The Guardian's* first disclosures in 2013, President Obama appeared on the Charlie Rose[1] show promising the American public that the NSA's protocols are transparent, and that US does not monitor the telephone calls or e-mails of its own citizens without a warrant or probable cause (Blanton, 2015). Shortly after, his own NSA review board concluded that: "the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks" (Clarke et al., 2013:104), adding 46 recommended changes concerning surveillance programs operating within the NSA. The board found that NSA data collection programs (specifically the telephone metadata collection program) were not only "ineffective" at stopping terrorism, but also illegal or unconstitutional in some cases (Clarke et al., 2013).

Uncovering the relationship between the new global empire of the tech world and intelligence agencies has been among the most significant Snowden revelations. On the one hand,

we see voluntary compliance from companies willing to adhere to government and crime investigations, handing over user information in exchange for court-ordered warrants. On the other, we see companies forced to give the NSA unlimited access to their servers, gag-orders prohibiting them from telling their clients, and hefty fines for non-compliance. For example, in 2007, Yahoo lost a legal battle with the NSA and was to be fined $250,000 per day for not giving up access to their servers through the PRISM program. They were also legally forbidden from alerting its clients of this breach of privacy (Rusche, 2014; Schneier, 2015). Earlier this year, we witnessed Apple's flat out refusal to cooperate with the state when they were asked to weaken their own security standards, in the highly-publicized case of *Apple v. FBI*. After a public relations showdown in which the FBI appeared to be losing, the FBI promptly dropped the case, suddenly claiming they could unlock the iPhone in question without Apple's help after all. Schneier has explained why inserting backdoors into encryption protocol exclusively for authorities is not a viable option:

> You can't build a backdoor that only the good guys can walk through. Encryption protects against cybercriminals, industrial competitors, the Chinese secret police and the FBI. You're either vulnerable to eavesdropping by any of them, or you're secure from eavesdropping from all of them (2014).

In a 2015 interview, Snowden expressed that any internet company that gets popular enough is certain to be approached by government forces for access (Hill, 2015), a statement which has also been articulated by Julian Assange in his book *When Google Met WikiLeaks* (2014). Some of the NSA slides themselves have shown that Google, Facebook, Apple, Microsoft, Yahoo, Twitter, Skype, Amazon and AOL have joined forces (however unwillingly) with the NSA by giving them direct access to their databases through the PRISM program[2]. Here, the *Washington Post* has reported on how NSA programs use tricky language to legally justify the collection of

American communications by using the word "incidental", implying that any US communications are accidently swept up in the surveillance of foreign targets and are thus fair game to collect:

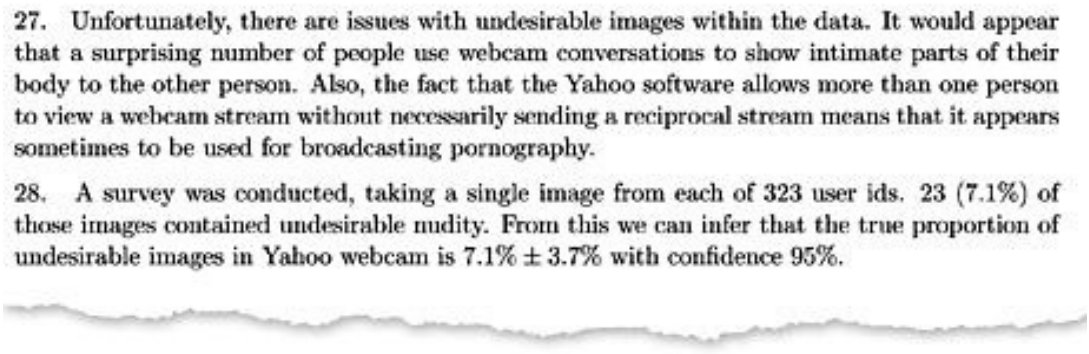
> Analysts who use the system from a Web portal at Fort Meade, Md., key in "selectors," or search terms, that are designed to produce at least 51 percent confidence in a target's "foreignness." That is not a very stringent test…Even when the system works just as advertised, with no American singled out for targeting, the NSA routinely collects a great deal of American content. That is described as "incidental," and it is inherent in contact chaining, one of the basic tools of the trade. To collect on a suspected spy or foreign terrorist means, at minimum, that everyone in the suspect's inbox or outbox is swept in. Intelligence analysts are typically taught to chain through contacts two "hops" out from their target, which increases "incidental collection" exponentially (Barton & Gellman 2013).

Further, the documents have also shown how the NSA intercepts communications through fiber-optic cables that make up the physical infrastructure of the internet via the UPSTREAM and MUSCULAR programs[3]. This is done through tapping undersea cables which is made possible through agreements with telecommunications companies (Ball, 2013). Because of these partnerships, David Lyon has explained that "much of the world's fiber optic cable is accessible to the US" (2015:145). Much to the dismay of the companies themselves, Snowden provided evidence of NSA hacks into Google and Facebook's databases without their knowledge via the MUSCULAR program even though they had already had access through PRISM. These types of collection can occur without individual warrants, court orders, user permission and without even alerting the companies involved (Mills, 2015; Schneier, 2015). Schneier has shed light on outrage in the corporate world, as products with weak security standards are undesirable commodities. Upon learning of NSA hacks into connections between their own data centers, Google and Yahoo have since responded by encrypting the data flowing between them (Schneier, 2015). Communications travelling through fiber-optic cables are also intercepted by the UK's GHQC through a program named TEMPORA; its contents are also shared with the NSA. TEMPORA[4]

works by intercepting digital communications as they travel across the Atlantic Ocean: The GCHQ mass tapping operation has been built up over five years by attaching intercept probes to transatlantic fibre-optic cables where they land on British shores carrying data to western Europe from telephone exchanges and internet servers in north America (MackAskill et. al, 2013).

Through other NSA programs, user efforts to remain anonymous online are also routinely subverted. In a program called EGOTISTICALGIRAFFE, the NSA attacked TOR users' computers through a vulnerability in older versions of Firefox. TOR (The Onion Router) is a software program used to search the internet anonymously by shielding IP addresses by bouncing them to exit routes in other countries. For example, to an outsider viewer, a TOR user in Canada may appear to be conducting internet research from an IP address in Brazil, whereas a user from Brazil may appear to be operating out of Germany (Ball, Schneier & Greenwald, 2013). President of the TOR project, Roger Dingledine asserts that the wide scale use of TOR is a great tool for subverting mass surveillance in general but cannot guarantee full protection from intelligence spying: "The good news is that they went for a browser exploit, meaning there's no indication they can break the TOR protocol or do traffic analysis on the TOR network…Infecting the laptop, phone, or desktop is still the easiest way to learn about the human behind the keyboard" (Ball, Schneier, Greenwald, 2013). As will be explored later, the strength in running TOR or other encryption programs for everyday use relies on the number of users. At least theoretically, making it more difficult for authorities to run dragnet operations on run-of-the-mill internet data forces them to engage in more traditional methods of targeted surveillance on suspects of wrongdoing due to a lack of resources.

One of the more disturbing documents in Snowden's roster pertains to a program called Optic Nerve. Over a six-month period in 2008, the NSA, in conjuncture with the GCHQ hacked the personal webcams of 1.8 million Yahoo users around the world. Unbeknownst to Yahoo, livestream videos and images of people in their own homes were secretly collected, and much of the content was explicit in nature (Ackerman & Ball, 2014). In the document, the users surveilled under this project were described as "unselected", meaning that this was a bulk collection program with no particular targeted individuals in mind. Rather than save full video streams, the GCHQ would save a screenshot every five minutes, "partly to comply with human rights legislation, and also to avoid overloading GCHQ's servers" (Ackerman & Ball, 2014). Later, the programs processed the images to experiment with facial recognition technology. OPTIC NERVE was still in effect by 2012. Although the GHCQ has limits on searching for individual data on anyone in the British Isles, they have no legal mandate to protect the privacy of Americans, Canadians, or citizens of any other country. Here lies the problem with data sharing between the Five Eyes alliance. In this example, the UK has no legal requirement to protect the privacy of Americans, but can easily share collected data with the US (Ackerman and Ball, 2014). The following image is an internal classified NSA document explaining the explicit nature of the images and videos collected wherein 7% of the OPTIC NERVE data contained nudity:



27. Unfortunately, there are issues with undesirable images within the data. It would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person. Also, the fact that the Yahoo software allows more than one person to view a webcam stream without necessarily sending a reciprocal stream means that it appears sometimes to be used for broadcasting pornography.

28. A survey was conducted, taking a single image from each of 323 user ids. 23 (7.1%) of those images contained undesirable nudity. From this we can infer that the true proportion of undesirable images in Yahoo webcam is $7.1\% \pm 3.7\%$ with confidence 95%.

As can be inferred from these documents, abuse of authority is all too easy. As Snowden has explained in various interviews, sharing nude images of internet users around the office happens regularly within intelligence communities (Schmidt, 2014).

Further, using the Snowden documents, Gellman & Soltani have explained how the NSA uses various programs under the codename CO-TRAVALER to track over 5 billion pieces of cellphone location data from all over the world: “Sophisticated mathematical techniques enable NSA analysts to map cellphone owners’ relationships by correlating their patterns of movement over time with thousands or millions of other phone users who cross their paths” (Gellman & Soltani, 2013). Another NSA program, XKEYSCORE, allows for searching the entire database of all the programs through keywords, IPs or email addresses. Snowden has shown that XKEYSCORE is used to sift through large quantities of data to find every piece of information on any given user or topic. According to Mills, the legal justification for XKEYSCORE remains a mystery (2015).

The idea of any institution conducing dragnet surveillance on entire populations can be considered a serious breach of privacy. Computer and cellphone connections are manipulated to collect users’ personal chats, e-mails, phone calls, internet searches or even the audio and video from inside their private homes. This breach of privacy is secretly conducted through technology

users have voluntarily purchased and from programs they willingly use. Their information is collected from social media databases, in transit through fiber-optic cables, and even sometimes intercepted from cellphones or laptops in real time. Constitutional rights in the United States and the Charter of Rights and Freedoms in Canada both safeguard citizens from unreasonable search and seizure without a warrant. However, since 9/11 a handful of intelligence agencies have decided to "collect it all" without the public's knowledge. What's most shocking is that since the Snowden disclosures, it is impossible to know which programs have remained functional and which have been revoked. Optimistically, I set up interviews to help find the answer to the question: "What does the current surveillance state of the US and Canada look like today?". To my surprise, each respondent replied with the same general answer, expressing the idea that nobody really knows, or that nobody can really say for sure due to the lack of transparency within surveillance culture. To catch even a tiny glimpse of what is happening within intelligence agencies of the Western world, the Snowden documents are some of the only available evidence with which to work.

## Authority, Transparency, Accountability

In an article titled "The Future of Privacy in the Surveillance Age", Jon Mills has helpfully outlined the civilian NSA spy programs and their features along with their legal justifications. The legal justification for these programs is often attributed to Section 702 of the FISA amendment based on the idea that "foreign targets do not receive constitutional protections" or Section 215 of the Patriot Act (Mills, 2015: 210-217). Cindy Cohn of the Electronic Frontier Foundation explains the role of Section 702 as the law that gives government access to digital communications through UPSTREAM and PRISM: "they travel the Internet backbone (called Upstream) and access to communications stored with service providers like Google and Facebook (called Prism)" (Cohn,

2016). Another justification often-used for these programs is that Americans should have no reasonable expectation of privacy when sharing data with third-parties (Mills, 2015: 210-217). As we will see, this precedent is based on a court ruling which was decided before the world-wide web even existed (Mills, 2015).

Due to the speed at which digital technology has developed over the past two decades, internet companies and intelligence agencies have been able to develop intrusive practices faster than laws can progress. The precedent set for determining Americans' reasonable expectation for privacy was set in the 1979 court case of *Smith v. Maryland*[5]. The ruling pertained to the unwarranted use of a pen register by law enforcement and deemed them not-constitutionally protected. The court ruled in favor of the state because customers should have "no reasonable expectation of privacy" when sharing information with third-parties. At the time, the only third-party involved was the phone company who kept call history records. According to the Supreme Court ruling, the Fourth Amendment was not violated because no search was technically performed, since call logs are already collected by the phone company (Mills, 2015:210). Since then, this interpretation of the law has been loosely used to justify government spy programs much more invasive and extensive than the collection of landline phone records. As the scope and volume of data made available to third-parties has dramatically transformed in the digital age, third-parties can include any website, internet service provider, application, etc. According to Mills, using *Smith v. Maryland* as precedent to support today's digital data collection is a prime example of the law's inability to effectively adapt to modern reality (Mills, 2015). However, not all judges agree that *Smith v. Maryland* is still relevant to today's world. In one particular example, the state used *Smith v. Maryland* in their defence of the collection of US citizens' phone call metadata in *Klayman v. Obama* (2013). In response, federal judge Richard Leon rejected the

precedent, referring to the bulk collection of American communications as “likely unconstitutional”. He went on to explain: "[T]he Smith pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones” (*Klayman v. Obama*, 2013, in Fidler: 2015: 224).

In general, surveillance reform has taken a baby step approach towards progress. Authorized by Section 215 of the Patriot Act, a telephone metadata NSA program has since been revoked after *ACLU v. Clapper*. Before the program’s expiration, the NSA had been collecting bulk metadata on US phone traffic, both foreign and domestic, unbeknownst to Congress or the general public (Wasserman, 2015; Schneier, 2015). However, according to DNI Hayden, the NSA still has access to phone call metadata, although they are no longer authorized to store it on their own servers: The lack of reform that has been imposed on intelligence agencies since Snowden has been openly mocked by Hayden in a publicly televised interview:

> If somebody would have come up to me and say ‘Look, Hayden, here’s the thing: This Snowden thing is going to be a nightmare for you guys for about two years. And when we get all done with it, all you’re going to be required to do away with is that little 215 program about American telephony metadata — and by the way, you can still have access to it, but you got to go to the court and get access to it from the companies, rather than keep it to yourself’ — I go: ‘And this is it after two years? Cool!’ (Froomkin, 2015).

Snowden also provided the press with a top secret internal NSA audit to reporters, proving that the agency abused protocol thousands of times in a single year, even by their own standards (Gellman, 2013). The NSA wasn’t the only agency caught red-handed; Snowden’s disclosures put other intelligence agencies under scrutiny as well. As it stands, intelligence agencies either have no oversight boards at all, so in Canada, they operate under secret courts appointed to oversee

intelligence programs which are neither transparent nor do they provide meaningful oversight. The FISC, the secret court put in place to monitor the NSA, only denied 11 requests out of 33900 in 33 years (Snowden, 2016B). Despite the FISA court's lenience, it also became clear that the NSA had also lied to them about the scope and purposes of their programs (Goodale, 2013; Gellman, 2013; Hewitt, 2015; Greenwald, 2014). Hewitt explains further while highlighting the importance of open discussion on the legality of mass surveillance tactics:

> Since 2006, FISC had believed it was approving interception of discrete communications of specific targets. In 2011, it realized entire Internet transactions were being collected, indiscriminately sweeping up mass amounts of domestic and untargeted data alongside each discrete target, yet the program had been regularly approved for five years without this central understanding. A process open to adversarial input would have forced FISC to confront this factual inaccuracy far sooner (Hewitt, 2015:73).

Rule-bending through omitting the truth, territorial legal loopholes, selective interpretations of language such as questionable use of the words "relevant to an investigation" and other questionable activities have allowed the Five Eyes and their partners to benefit from sharing data from each other's countries, and giving them access to "almost everything" in terms of digital information (Schneier, 2015:59). While the partnership was originally purposed to help each other with foreign espionage in WWII, the new purpose of the Five-Eyes is to aid each other with domestic surveillance initiatives (Farrell, 2013). Not only is it difficult to keep track of where data flows and where it is stored across the globe, but intelligence agencies subcontract their work to other security companies, making it tough to know who is conducting surveillance and for what purposes (Lyon, 2015). According to Schneier, almost 2000 corporations deal with homeland security and counterterrorist programs in the Unites States alone (2015).

A lack of public understanding of digital era surveillance combined with loose or non-existent regulations surrounding user privacy created the perfect recipe for the abuse of power and

resources. In these times of low government transparency and accountability, Snowden represents a beacon of light in the era of "guerilla accountability" (Whitaker, 2015), alongside WikiLeaks, Chelsea Manning's classified military leaks, Hilary Clinton's publicly exposed e-mails, the Panama Papers and the Drone Papers, to name a few. According to Whitaker, this guerilla accountability via leaks and whistleblowing is due to a lack of government and corporate transparency in various political arenas. As a result, these actions should be seen as a response to the absence of public awareness, lawful conduct or meaningful oversight (Whitaker, 2015). For this reason, many others have argued that whistleblowers need better legal protection and channels to leak information as well as to defend their actions in a court of law (Schneier, 2015). This is not to say employees handling sensitive documents should leak anything and everything without consequences, but that they should have access to fair public trials. In the instances that national security was not, in fact, put at risk, and as long as appropriate safeguards were put in place to avoid putting others in danger, whistleblowing is one of the only ways to effectively expose government or corporate wrong-doing. For that reason, whistleblowers, even those charged under the Espionage Act, should be permitted to make their case before a jury of their peers in order to be judged on whether or not their actions were justified in the name of public interest.

## The Terrorist Threat

Despite being justified by counterterrorist legislation, foreign intelligence and national security, intelligence programs use their extensive data collection capabilities for many other purposes. For example, Facebook and e-mail information collected in the name of national intelligence and counterterrorism trickles down to other law enforcement entities where they are subsequently searched for other types of criminal activity. In 2015, a Foreign Intelligence

Surveillance Court (FISC) ruling concluded that information accessed by the NSA in the name of national security would also be legally accessible to the FBI for local crime investigations. According to the FISC, NSA mining of digital communications is protected under Section 702 provided that national security is the primary reason for collecting the data. After that, the warrantless search and use of said data is fair game in other agencies such as the FBI who may be looking for other types of criminal evidence. Here, it is irrelevant whether or not the targets are within the US because FISA operates outside of constitutional rights to privacy for Americans:

> The upshot is that the government needs a national security or foreign intelligence purpose only for the initial collection and analysis of information. Once it has communications in its custody, those limitations no longer apply and the government can troll through it for whatever law enforcement purpose it wants without having to worry about getting a pesky warrant (Cohn, 2016).

Even on the grounds of counterterrorism, critics argue that support for civilian spy programs and tactics are at best, ineffective, and at worst, detrimental to human rights and democratic values. NSA director Keith Alexander defended the NSA's bulk collection of telephone data by insisting it had foiled 54 terrorist plots. To quote Thomas Blanton, director of the NSA archive at George Washington University: "only 13/54 [terror plots] were connected to the US… the bulk telephone metadata program had broken no such plots, and only identified a single terrorist whom the FBI was already tracking" (Blanton, 2015:289). The threat of terrorism itself is also exaggerated; as Schneier says, in the US, the probability of being killed by a police officer to being killed by a terrorist is 9:1 (2015). In his 2016 essay on political resistance, Snowden argues that this extreme focus on terrorism is a way of obtaining social control through fear mongering. Snowden asserts that the state is pouring too many resources into stopping terrorism while there are much greater threats to human life: "…recognize that even if we had a 9/11 attack every year, we would still be losing more people to car accidents and heart disease, and we don't

see the same expenditure of resources to respond to those more significant threats" (Snowden, 2016A). Furthermore, some argue the NSA's inability to prevent 9/11 wasn't an issue of having access to enough data or the inability to connect the dots. Blanton has stated that without the extreme culture of over-classification and secrecy within the CIA and the FBI, they might have been able to prevent the attacks (Blanton, 2015). Along these lines, even Jim Sensenbrenner, the author of The Patriot Act (the legal justification of the existence of many bulk collection NSA programs), has admitted that the process of collecting "the haystack" causes authorities to miss cues, which he attributes to the reason why the Boston bombers were able to slip through the cracks despite bulk collection programs (Fox, 2013).

Upon learning of the true usage of NSA programs via the Snowden files, Sensenbrenner aided in *ACLU v. Clapper* (2015)[6] because of his own disbelief at the NSA's loose interpretation of the act. He argued that if he, or Congress, had been aware that the act would be used to monitor every single cellphone call within the United States, they would have objected. The Privacy and Civil Liberties Board (PCLOB) also found that "Section 215 metadata vacuum cleaner was illegal, ineffective and unconstitutional" and "secrecy had completely undermined the constitutional checks and balances" (Blanton 2015: 290). After the expiry of the Patriot Act, Sensenbrenner introduced the USA Freedom Act as part of a surveillance reform to impose new limits on the bulk collection of American metadata. Though critics argue the new law is not extensive enough, one of the limits the USA Freedom Act requires is that the NSA now has to ask for permission for data from phone companies instead of collecting and storing it at their own leisure (Froomkin, 2015).

The same fear-based arguments are also used to weaken encryption standards in order to give up warrantless access to digital communications: "That's the NSA's justifications for its mass

surveillance programs: if you let us have all of your data, we'll relieve your fear" (Schneier, 2015). Timothy May, author of *Crypto Anarchy and Virtual Communities* (1994*)*, has coined the phrase "the four horsemen of the infocalypse" to refer to the dangerous or offensive groups such as terrorists, drug dealers, child pornographers etc., who are often cited as the reasons why that general population should be denied access to encryption. May uses the concept of free speech to backup the ideological right to securing data: "The basic right of free speech is the right to speak in a language one's neighbors or governing leaders may not find comprehensible: encrypted speech" (1994). The basic idea is that even though criminals and other bad actors may be using the internet to meet their own ends, it should not give the state the right to search the entire population's communications. Just as the police are not legally allowed to search private property without a warrant just because some houses may contain illegal materials, the state should not have warrantless access to every single online action because some users are behaving illegally (Schneier, 2015). Amnesty International[7], The Electronic Frontier Foundation[8] and other digital rights advocates, including social theorist Ulrich Beck (2013), have argued that encrypting and protecting data should be regarded as a fundamental human right. Further, Gill, making reference to ideas from Peter Swire (2011) and others, argued that even if all digital transactions were encrypted, the state would have still an unprecedented amount of access to information on the public's communications through metadata alone (Interview data, 2016). Moreover, as a democracy, even if the American public willingly consented to the warrantless collection of all communications with the end goal of stopping terrorism, the questions of authority abuse and the misuse of programs still remain.

## Oh, Canada

In Canada, John Forster, chief of the Communications Security Establishment (CSE) was quoted by the CBC in saying: "We do not target Canadians at home or abroad in our foreign intelligence activities, nor do we target anyone in Canada…In fact, it's prohibited by law. Protecting the privacy of Canadians is our most important principle" (Wetson et al., 2014). The Snowden documents have suggested otherwise. In one example, Greenwald collaborated with the CBC to report on CSE's unlawful tracking of thousands of cellphone users for two weeks after visiting a Canadian airport[9]. In response, the Harper administration dismissed the reports as false, despite Snowden's internal CSE documents which clearly display the results of the programs. In a curious attempt to discredit Greenwald's character to the House of Commons, parliamentary secretary Paul Calandra not only rejected the journalistic integrity of the CBC for working with him, but also referred to Greenwald as a "porn spy" out to line his "Brazilian bank account" (Greenwald, 2014).

In another example, the documents showed how the CSE's LEVITATION program monitors millions of Canadian downloads and uploads per day (Geist, 2015). Citizen Lab's Ron Deibert has commented on the document: "Every single thing that you do – in this case uploading/downloading files to these sites – that act is being archived, collected and analyzed" (Gallagher & Greenwald, 2015). The internal CSE PowerPoint slide showed that not even .0001% of what they collect through LEVETATION to be relevant to any investigation or suspicious activity (Gallagher & Greenwald, 2015). Using these program, CSE agents are able to correlate IP addresses with e-mail addresses, Google analytics cookies and Facebook profiles to create a digital map of the online activity of any individual. The CSE's involvement with civilian spy programs contradict basic Canadian values reflected in Section 8 of the Canadian Charter of Rights

and Freedoms, which is the right to privacy against unreasonable search or seizure. Before Snowden, Canadians had no way of knowing about the collection of their data, much less the opportunity to engage in meaningful debate over the use of programs which facilitate it.

Since Snowden, Canada has added more extensive powers to their surveillance agencies. In my interview with Aaron Thaler, founder of the Student Coalition for Privacy in Montreal, I asked him about his organization's mission to mobilize Canadians against Bill C51. Bill C51, or the Anti-Terrorism Act, became law under Harper's Conservative government in the summer of 2015. The law gives more sharing powers to various government sectors. For example, information on Canadians can now be shared between the RCMP, CSE, Health Canada, border services, or Canada Revenue Agency in ways that were not legal before. The most problematic aspect of C51, says Thaler, is that it also increases policing powers of intelligence agencies. In Canada's not so distant past of the late 60s and 70s, the RCMP had abused their spy powers, resulting in the McDonald Commission which separated intelligence gathering from policing with the formation of CSIS (Canadian Security Intelligence Service). Today, Thaler explains how C51 gives expands CSIS capabilities: "it gave them police powers like intervention powers, interference powers, the ability to censor online websites...CSIS was created to separate the law enforcement powers from intelligence powers of the RCMP. So what bill C-51 does is the opposite, it undoes this" (Interview data, 2016).

Though the Liberal Party of Canada has promised to amend Bill C51, it has been in effect as law since the summer of 2015. C51 allows the police more leeway involving warrantless arrests, referring to "interference with critical infrastructure" as a threat to national security. The law's expansion of information sharing and policing powers combined with vague definitions of terms

like “terrorist propaganda” have alarmed those sympathetic to environmentalist groups and other peaceful protesters that may potentially be deemed terrorists (Watters, 2015). In an open letter to parliament, over one hundred Canadian law professors and legal experts protested the bill: “We believe that terrorism must be countered in ways that are fully consistent with core values (that include liberty, non-discrimination, and the rule of law), that are evidence-based, and that are likely to be effective” (Abell et. al, 2015). Here, C51 is used as an example of the expansion of mass surveillance at a time where meaningful public dialogue about privacy is finally coming to fruition.

As previously mentioned in the case of data sharing between the NSA and the GCHQ, Five-Eyes data sharing works around territorial laws, while it’s perfectly legal for foreign countries to spy on Canadian communications because the Canadian Charter doesn’t apply to foreigners. Allied countries like the United States can collect information on Canadians and feed it back to Canadian intelligence, thus benefiting from a legal loophole whereby Canada is receiving information on their own citizens from countries not bound by our laws. In turn, Canada also shares data they’ve collected on the citizens other Five-Eye partners with them. In the Canadian context, legal expert Michael Geist has written about the need for law and policy reform in order to reflect the digitally advanced world we live in: “the legal framework leaves Canadians with twentieth-century protections in a world of twenty-first-century surveillance” (Geist, 2015:249). In the contemporary context, even safeguards put in place to localize Canadian data in response to recent privacy concerns may be unraveled by the TPP which seeks to revoke efforts to keep Canadian data within the jurisdiction of the country (Geist, 2015a).

The way data flows across borders makes laws confined within psychical spaces easy to avoid. These capabilities become particularly alarming when intelligence gets it wrong. In my

interview with Thaler, he explained how the consequences of data sharing can be life-changing for the victims involved. He gave the example of Maher Arar, a Canadian citizen who was deported back to Syria while visiting the US in 2002. Arar was subsequently tortured in Syria based on false information the Canadian RCMP provided to the CIA. According to reporting from the CBC: "He has described a year-long ordeal that included being beaten and stuffed into a body-sized slot in a windowless dungeon. Arar likened it to being buried alive" (Panetta, 2015). After recognizing he was not affiliated with al-Qaeda after all, the Canadian government has since allowed Mr. Arar back into the country and have since issued him an 11.5-million-dollar settlement (MacCharles, 2007). The fear of legislation that expands the surveillance and policing powers of the state, such as Bill-C51, is grounded in this type of anecdotal evidence. Mr. Arar is a prime example of how easily the sharing of faulty information can go terribly awry.

In the summer of 2016, another case of faulty information sharing within the Five-Eyes has made the news. New Zealander Tony Fullman's home was raided and his passport wrongfully revoked in 2012. This time, the mix up was due to misinterpreted information collected via the PRISM program which the NSA then provided to New Zealand intelligence. Because Fullman had "liked" the Thumbs Up for Democracy page on Facebook, his private e-mails and Facebook messages were collected via PRISM and shared with the New Zealand's Government Communications Security Bureau (GCSB). In the end, Fullman, an advocate for Fijian democracy was wrongfully accused of plotting a terror attack against the state by his own country (Gallagher & Hager, 2016). Fullman's case is of particular importance because it is the first time the public has gained knowledge about an actual person targeted with the PRISM program. Based on the relentless reporting of Snowden documents and related issues from *The Guardian* and other media outlets, we can most likely expect to see similar examples pop up in the near future.

## Metadata

According to the Statement from the Minister of National Defense on the CSE Commissioner's Annual Report for 2014-2015[10], one legally problematic activity identified in the oversight of the CSE was metadata sharing. Allegedly, Canadian metadata was accidentally being shared with foreign allies without safeguarding individual identities:

> CSE discovered, on its own, that certain types of metadata were not being properly protected prior to sharing with allies, due to technical deficiencies in CSE systems. CSE proactively informed the Commissioner about these matters, and suspended the sharing of this metadata to Canada's partners. The Commissioner has since concluded the legal assessment associated with this review and reported his finding to me and the Attorney General of Canada. The metadata in question that was shared with Canada's partners did not contain names or enough information on its own to identify individuals. Taken together with CSE's suite of privacy protection measures, the privacy impact was low. I am reassured that the Commissioner's findings confirm the metadata errors that CSE identified were unintentional (Sajjan, 2016).

Downplaying metadata as an invasion of personal privacy is a controversial endeavor. The reason is because metadata is a term often used to downplay the significance of the types of data being collected. Examples of metadata are what IP addresses visited what websites, or logs of what phone calls were made from a specific number. The popular defense of metadata collection is that it is not invasive because it cannot be linked back to individuals, since it does not provide any content, only context. For example, in *Data and Goliath*, security expert Bruce Schneier references former NSA General Counsel Stewart Baker to illustrate the capacity of metadata to divulge private information: "Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content" (2015:22). Even worse, former NSA and CIA director Michael Hayden has been quoted as saying: "We kill people based on metadata" (Schneier, 2015: 22). More importantly, the problem here extends well beyond collecting and sharing metadata which has not been properly secured to ensure anonymity, as Snowden's

documents have outlined the ways in which intelligence agencies associated with the Five Eyes most certainly do collect the content of communications in mass quantities as well (Mills, 2015; Greenwald, 2014; Schneier, 2015).

The reach of surveillance programs underlined in this chapter demonstrate the logic behind the post 9/11 goal of "collecting the haystack" in regards to digital communications. To be sure, while citizens should be able to maintain a certain level of privacy, so should the government that works to represent their interests. The argument presented here is not that we need one hundred percent transparency at all levels of government, but that a democratic public should have the ability to engage in meaningful dialogue and discussion surrounding acceptable methods and levels of surveillance before they are set into motion. The purpose of this chapter has been to investigate the capabilities of some of the programs identified through the Snowden documents released by the media. We have explored the realities of data mining, counterterrorism, cross-territorial data sharing, and some of the legal justifications of mass surveillance in both Canadian and American contexts. We have also shed light on how the data-sharing protocols between the Five Eyes undermines legal boundaries and constitutional rights, and the ways in which wrongly-accused people are effected by policing by intelligence programs. In this chapter, we have provided a preliminary map of some of the most popular Snowden documents along with the political debates that come with them.

---

[1] See the video here Obama Defends NSA Surveillance Programs – Charlie Rose https://www.youtube.com/watch?v=dRvrFVxvB3I

[2] PRISM document http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

[3] MUSCULAR document http://cryptome.org/2014/01/nsa-sso-dk.pdf

[4] GCHQ's Tempora http://www.spiegel.de/media/media-34103.pdf

[5] *Smith v Maryland*, 442, US 735, 743 (1979)

[6] *ACLU v. Clapper* Amicus Brief https://www.eff.org/document/aclu-v-clapper-amicus-brief

[7] See https://www.eff.org/deeplinks/2016/03/amnesty-international-encryption-human-rights-issue

[8] See https://www.eff.org/deeplinks/2015/06/un-special-rapporteur-calls-upon-states-protect-encryption-and-anonymity-online

[9] Airport wifi surveillance document http://www.cbc.ca/news2/pdf/airports_redacted.pdf

[10] Statement from the Minister of National Defense on the CSE Commissioner's Annual Report for 2014-2015https://www.cse-cst.gc.ca/en/media/media-2016-01-28

# Chapter Four

## Cyber Optimism and Encryption as Risk Management

Following Edward Snowden's revelations concerning the surveillance programs of the Five Eyes, we have come to understand insecure telecommunications networks as channels for deep-seated exploitation and privacy invasion. This chapter uses interview data to explore the role of software development and activism in protecting privacy communications. Here, encryption can be considered a risk-management solution for securing online content from prying eyes. As we have outlined in the previous chapter, some US legislation, such as the Patriot Act, has also slowly begun to shift since 2013. According to Reitman of the Electronic Frontier Foundation (EFF), in an attempt to regulate unwarranted government surveillance, the Snowden leaks aided in pushing the USA Freedom Act[1] into action, which replaced the Patriot Act and put new limits on NSA bulk collection as "the first piece of legislation to rein in NSA spying in over thirty years" (Reitman, 2016). The leaks also helped spark congressional policy debates about FISA court powers, specifically section 702 of the FISA Amendments Act, a subsection of the law which is largely responsible for NSA's catch-all surveillance tactics which will expire next year. Reitman highlights the fact that official government responses to Snowden's documents have served as evidence in court cases challenging NSA programs: "The Snowden leaks and statements made by public officials responding to the leaks corroborated and provided vital details about NSA surveillance practices, which we're using in our court cases" (Reitman, 2016). Though this can be considered a small step towards a big social change, there is still much more to be done.

In Canada, privacy law and policy reform is also necessary to protect digital rights, as has been proposed by Michael Geist. In this view, the privacy commissioner's plans to implement

oversight boards to watch over the lawful-but-unjust programs of the Canadian Security Establishment (CSE) is a Band-Aid solution to fixing such deep-seated issues (2016). However, waiting for extensive policy and legal reform is not the only option for securing digital data. Outside of official government channels, there are many types of groups and actors working to limit the range of mass surveillance. For our purposes, digital activism can be defined as any action deliberately intended to disrupt state surveillance on the internet. Some of the ways of doing this are: disguising or obfuscating communications data (Brunton & Nissenbaum, 2015); developing or using encryption software; mobilizing protesters through signing petitions or other means; raising public awareness through social media and journalism; and even through DDoS (denial-of-service) attacks, which is the strategy hacker-group Anonymous used to take down Canadian government websites in response to the introduction of Bill C-51 in 2015.

To place Snowden into a broader historical context of protecting the internet in a battle that precedes his intervention by a few decades, it helps to consider the larger movement at play. Crypto wars began in the 1970s when the US government tried to regulate or interfere with the use of encryption in universities (Foundation for Information Policy Research, 2005). Here "the crypto war" refers to the ongoing power struggles between governments and activists, software developers and their competitors, between corporations and governments, intelligence agencies and law enforcement, and policy makers on the right to use strong encryption. In the 1990s, the Clinton administration failed to implement the Clipper Chip, which required industries to insert a backdoor to all encryption software, which would give the government access to any locked communication. It also failed to implement key escrow, which would allow a third-party to have a pair of all encryption keys that could be made available to the FBI upon request. These failed attempts at regulating encryption alongside Zimmerman's PGP (Pretty Good Encryption) publicly

accessible encryption software signified the end of the first crypto war. The outcome of this "war" was in favour of internet advocates despite US government initiatives to limit or control the use of encryption (Foundation for Information Policy Research, 2005). In lieu of the Snowden disclosures outlining NSA attempts to weaken commercial encryption standards and in reference to the resurgence of debates regarding cryptography use in general, Bruce Schneier has recently published a blog titled "The History of the First Crypto War"[2]: "The Second Crypto War is going to be harder and nastier, and I am less optimistic that strong cryptography will win in the short term" (June, 2015).

However, cryptography supporters and digital privacy advocates are not going down without a fight. The second wave "crypto war" is backed not only by monumental activist organizations such as the Electronic Frontier Foundation (EFF), Privacy International and Amnesty International, but also by corporate actors in Silicon Valley looking to protect their own public reputations. In one salient example, Apple refused the FBI's request to unlock the iPhone of one of the San Bernardino shooters after his death in the highly-publicized case of *Apple v. FBI (2016)*[3]. Since Snowden, arguments for privacy and the right to encryption have only become more focused and articulated by activist groups aiming to reform the internet and protect digital rights (Gill et al., 2015). Various hacktivists, whistleblowers, software developers, cryptographers, and journalists work together and independently to evade the effects of the panoptic gaze. These actors consciously make efforts to challenge surveillance through examples of defiance and dissent. In the name of civil liberties such as freedom of speech and the right to privacy, there are also many organizations, legal teams, and researchers working to create a more politically progressive and socially inclusive digital environment for everyone. These efforts include everything from pirating

digital content, to making the internet more accessible to the global population, to developing and promoting communications software which uses encryption by default.

From the early beginnings of world wide web in the early 90s, in a display of what Morozov calls "cyber-utopianism" (2011), techno-optimists have expressed deep faith in the internet as a potential equalizer of power relations, connecting the globe in a giant information-sharing network of knowledge exploration and communal values. Famously, John Perry Barlow's "Declaration of the Independence of Cyberspace" outlined these sentiments in 1996. In his declaration, Barlow deemed the internet a space outside of traditional borders, ultimately warning that state governance has no business in the unchartered territories of the internet. The declaration starts: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather" (1996). Under this ideology, as the internet becomes increasingly commodified and simultaneously equipped for mass surveillance, what we've seen so far is a gross misuse of its full democratic potential as a channel for information sharing, intellectual exploration, and anonymous discourse.

Barlow's dream is one shared by many internet advocates, activists and hackers for a wide variety of reasons. From his 2014 TedTalk entitled "Here's How We Take Back the Internet", we can infer that Snowden's version of cyber-optimism lies in the hope that the public will become empowered by the information he has shared and work towards gaining control of the internet at large as well as their own communications (Snowden, 2014). Though Snowden's self-proclaimed goal may have been to spark a public debate around digital privacy, the goal behind this type of activism is to reform intelligence agency protocols alongside the global expansion of privacy rights

in one giant leap towards internet sovereignty. Other actors working towards the idea of taking back the internet include those who believe in the potential of digital communities as expressions of anti-hierarchical and collaborative spaces; those against the state censorship of ideas and content; and digital pirates who evade laws by distributing various types of copyrighted files across networks. Following Barlow, in "You Are Not Welcome Among Us: Pirates and the State," Beyer and Mckelvey argue that while digital piracy is often associated with a movement against private property and copyright law, "digital pirates and broader 'hacker culture'" can more aptly be described as a challenge to state power in general (2015:890). Though various movements involving Internet freedom fighting have distinct differences, many of them can be generally understood as opposing forces against the highly-regulated creation and distribution flows of creative content under capital (Beyer & Mckelvey, 2015: 890).

More evidence that activist groups and program developers work to evade state power lies in the development of methods to escape the gaze of corporate and government surveillance through virtual private networks that allow for anonymous browsing, ad-blockers that challenge the corporatization of the web and disable online tracking, and the surge of applications that use encryption to protect in-transit messages between users. The development and use of encryption as a default means of communication is one technical solution agreed upon by various groups under a larger movement: "Activists, anarchists, and libertarians have tried to evade the state online. Hacker cultures associated with public cryptography (Zimmermann, 1999), cypher punk (Hughes, 1993) and crypto-anarchists (May, 1992) have all been inspired to develop better privacy communications for citizens (see Ludlow, 2001)" (Beyer & Mckelvey, 2015: 894). Here, the future of the internet lies in the actions and online habits of its users as well as the companies they decide

to support or boycott. For example, web-based companies and users may decide to support strong encryption, rendering non-privacy-compatible technology undesirable or even obsolete.

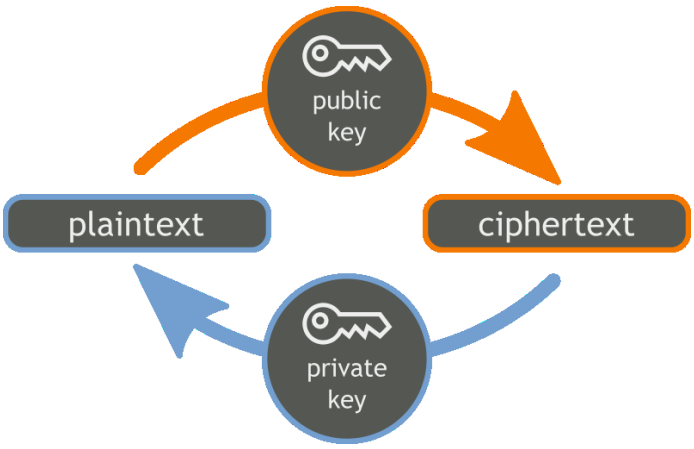
Another argument in support of widespread encryption is that it would theoretically force intelligence agencies and law enforcement to target specific individuals as opposed to collecting unprotected data on the population at large. In short, in terms of resources, if all digital content were encrypted, it would be too costly to attempt to crack millions of encrypted communications daily (Schneier, 2015). Although the promise of quantum computers threatens to undermine the strength of encryption as we know it, today's technology still makes it far easier to hack a computer or endpoint than to decrypt any protected message in transit. The unwavering flow of WikiLeaks' classified releases and the fact that the unpublished Snowden documents are still safely secured serve as evidence that properly implemented encryption works.

But how can we know which programs to trust? Supporting open source programs (programs whose codes are readily available for public verification and modification) is important because they compete with for-profit companies with hidden coding used to spy on unprotected user data to sell it to other companies for various purposes. TOR, although initially developed by the US government, is a free and open source program that uses encryption to hide the IP address of the user in order to secure private web browsing[4]. Dingledine argues that while TOR may not perfectly shield users from NSA spying, they must be pickier about who to target in order to not alert too many users at once: "TOR still helps here: you can target individuals with browser exploits, but if you attack too many users, somebody's going to notice. So even if the NSA aims to monitor everyone, everywhere, they have to be a lot more selective about which TOR users they spy on" (Ball, Schneier, Greenwald, 2013). Signal is a free and open source messenger application

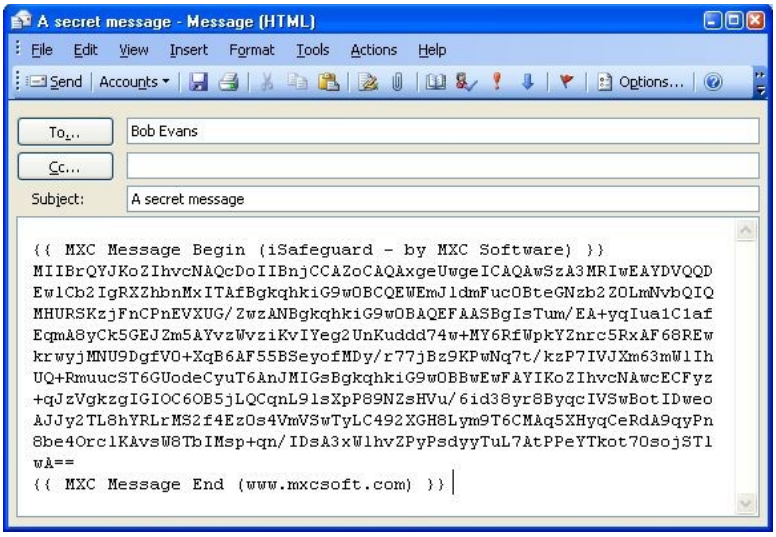
that has been verified by digital communities to ensure the reliability of its default end-to-end encryption. Using e-mail encryption programs is another way of securing digital messages from prying eyes. The idea is that every time internet users use encryption software for run-of-the-mill messages or internet browsing, the less often encrypted texts are reflagged as criminal, secretive, or politically active in nature. For example, this allows for the possibility of private messages between journalists and whistleblowers or other controversial sources to continue to flow without being targeted for extra surveillance. The following subsection includes a technical explanation of how encryption works and other reasons why we should use it.

## What is Encryption?

E-mail encryption is easy enough to use once the proper software is installed, but its inner workings are complicated to explain. PGP was developed for user-friendly encryption that makes messages such as e-mail content illegible to anyone without the proper set of keys. The private key, which is a long, complicated passcode chosen by the user connects with their public key, which is an even longer and more complicated combination of numbers and letters that is randomly generated. When users set up their encryption software for the first time, they create both a public and private key, a personal keyset which is unique to them. This key-generating process is one of the most important steps, and it only needs to happen once. To communicate using PGP, both parties must be using encryption, which is referred to as end-to-end encryption. Both of the public keys are known to both parties, while the private key is only known to the user trying to decrypt (or unscramble) the message at hand.




One way to think about it is that the public key is a device that scrambles the message turning the plain text into ciphertext (a randomized series of numbers and letters) on one end, while the private key is used to unscramble, or decrypt, the message on the other end, turning the ciphertext back into plain text. This way, third parties (Google, the NSA, independent hackers, or anyone else) cannot intercept the message while it's in transit; a message that says "Hi, how are you", would look like this until decrypted by the private key:




The rationality behind supporting strong encryption is as follows: properly implemented strong encryption is basically impossible to crack because it would take too long to do so due to

the complexity of lengthy mathematical equations. What makes PGP an important tool for privacy advocates is that encryption software uses math problems so strong that even the world's fastest computer would take an inconceivably long amount of time to crack one message secured with strong encryption. According to Bruce Schneier, expert cryptographer and author of *Data and Goliath: The Hidden Battles to Collect your Data and Control your World:*

> There's an enormous inherent mathematical advantage in encrypting versus trying to break encryption. Fundamentally, security is based on the length of the key; a small change in key length results in an enormous amount of extra work for the attacker. The difficultly increases exponentially. A 64-bit key might take an attacker a day to break. A 65-bit key would take the same attacker twice the amount of time to break, or two days. And a 128-bit key--- which is at most twice the work to use for encryption --- would take the same attacker…one million billion years to break. (For comparison, the Earth is 4.5 billion years old) (Schneier, 2015:104-105).

As a constitutional lawyer, political activist and journalist for *The Guardian*, Glenn Greenwald, was approached by Edward Snowden via e-mail in 2013. In Greenwald's book, *No Place to Hide: Edward Snowden, the NSA, and the Surveillance State,* he explains how Snowden wrote ambiguous messages to him under the pseudonym "Cincinnatus", promising that he had some very important information to share with the press that was too risky to divulge without using PGP. With no way of knowing that Snowden was an NSA contractor hoping to share millions of classified documents with him, Greenwald dragged his heels on downloading the encryption software, finding the installation process too daunting. Feeling frustrated after six months of waiting, Edward Snowden finally sent him a tutorial video on how to use PGP before the two could finally communicate. Shortly after, they met in Hong Kong where Snowden would pass the leaked NSA documents to Greenwald on encrypted SD cards. Today, Greenwald has written countless articles and best-selling books on the topic of digital rights and travels the world explaining the

significance of e-mail encryption to his audiences. Greenwald explains the significance of this further:

> The program essentially wraps every email in a protective shield, which is a code composed of hundreds, or even thousands, of random numbers and case sensitive letters. The most advanced intelligence agencies around the world —a class that certainly includes the National Security Agency—possess password-cracking software capable of one billion guesses per second. But so lengthy and random are these PGP encryption codes that even the most sophisticated software requires many years to break them. People who most fear having their communications monitored, such as intelligence operatives, spies, human rights activists, and hackers, trust this form of encryption to protect their messages (Greenwald, 2014:5).

## Interviews

To further explore the complexity of the intersection of technology and the law, I interviewed four researchers around the Montreal area with expertise in this area. As Gill explained in our interview, understanding the way encryption works is essential when advocating for digital privacy rights from a legal standpoint. For this reason, selecting proper metaphors to describe cryptography is crucial to legal debates, such as the controversy surrounding legally compelled decryption. While May (1996) has compared the right to encryption to the right to speak an unintelligible language outside of third-party comprehension, Gill has pointed out that the ACLU and EFF have tried to present encrypted messages as coded language, as opposed to other metaphors such as messages locked in a box (Interview data, 2016). For example, if the state wanted to convince a judge to legally compel someone to decrypt their messages and likened them to letters locked in a box, they could simply cite precedent of authorities gaining warranted access to locked boxes in the "real world". However, if the judge understands encryption as coded language shared by two actors, making a case to force them to translate their communications is

no easy feat, especially if the coded information could be used as incriminating evidence against them. It is important to remember, however, that encryption is not perfect, as the metadata about encrypted communications, i.e., who is contacting whom and when, is still viewable by third-parties. A hacked computer may allow the attacker to see the decoded message after it has been encrypted, even though it would be nearly mathematically impossible to decode in transit. Still, programs and platforms which use encryption by default are currently the best option for protecting communications from unsolicited third-parties.

As politicians and corporate leaders wrestle for power over rights to access and control internet users' online lives, we are smack in the middle of what is referred to as the "second crypto war". During his introductory speech at the crypto party, Dmitri Vitaliev, the founder and director of eQualitie, told the audience that "we won the first crypto war", so internet users need to start taking advantage of encryption software. The audience was there to learn how to use PGP in a free and informal workshop. When I asked him what he meant about winning the first war during our interview, he responded:

> Yeah, well I mean we won the war by the very fact that the (encryption) protocols were released, and again, once you release it, you can't take it back. It will always exist, the mathematical complexity that is involved in breaking those protocols remains, it doesn't matter if anybody knows about it or not. So this will always be something we have, in that way we won, yeah. We won the ability to use it and now we need to get the right to use it and we need to get people to actually use it. (Laughs) That has always been… I mean… that third thing almost always makes everything else irrelevant, we can do it, we have the tools and now let's do it.

Now that the math behind encryption has been publicly released, Vitaliev's idea is that internet users and software developers have to fight for the right to be able to keep using it. And, most importantly, more people have to start using it, which is why eQualitie and other organizations throw crypto parties for the public. While it may be up to software developers

to shape our online experiences, it is also up to the public to decide what types of organizations they'd like to support. To name an example, Duck Duck Go is a search engine similar to Google that doesn't track its users. The recent popularization of new companies that use encryption by default is promising, and companies like Google and Yahoo have started to encrypt data flowing between their servers to protect their data as well as their public image. The more users that start implementing encryption into their daily online routine will result in more companies supporting strong encryption as part of their business models. Ultimately, this will make it harder for the state to gain control over the right to strong encryption.

Vitaliev's answer also sheds light on a second noteworthy subject, namely, how the technologically literate need to find ways in which to engage the less digitally-advanced majority in order to have them join the privacy battle. For him, educating the public is key, as "no specific program can save us", it's the way in which we use and develop software and use protocol that can secure communications or leave them wide open. Similarly, Vitaliev mentioned that the Snowden documents persuaded many people to get involved in the movement to keep communications secure. For example, five years ago, he couldn't get people to come to his crypto parties, however, more recently, eQualitie has hosted parties packed with people eager to learn how to encrypt their e-mails. Though this new surge of interest in private communications is progressive, he believes there is still much work to be done. Vitaliev's mission as an activist is all about getting the general public to understand not only technology, but the laws and policy behind private communications, surveillance, and digital rights. His organization also develops encrypted chat software and fends off attacks from malicious hackers for their clients, some of which include websites for the LGBTQ community in hostile countries. He explains how he has seen a shift in the software industry since Snowden's debut:

> So I think for us it's a big battle along with the battle for the right to use encryption which is the next step of the surveillance world. Because, again, the Snowden leaks have led to a lot of developers leaving their jobs and joining the types of organizations that we're running. There have been a lot of tools being developed… so now that we have more hands and more eyes and more heads working on making tools better we have to consider what about the protocols? Are they gonna let us use these protocols? (Interview data, 2016)

Snowden's work has motivated more developers to join the movement by helping to build tools that help internet users privately communicate. Many software developers have left the corporate world to work with non-profit organizations like eQualitie after the Snowden revelations, and they have taken a pay-cut to do so. For Vitaliev, now that we have the protocols, the key to civil liberty is developing even better user-friendly software getting the general public to comprehend what's at stake in terms of privacy rights. In order to do so, we also need a deeper understanding of where corporate and government policies fit in to the equation. The hope is that through expanding the public's knowledge on these issues, strong encryption can be standardized and protected through new legislation.

On the other hand, Thaler argues that putting the responsibility on users to protect their own data is challenging because it creates a situation where the technologically-literate are able to evade certain types of surveillance while others cannot. Further, even those with high computer literacy may not fully understand the political implications behind strong encryption and opt not to use it. In order to make secure communications equally accessible to all users, software developers should focus on creating user-friendly programs that use encryption by default. Thaler has shed light on this topic by advocating for applications that automatically encrypt content and by arguing for doing away with e-mail all together since using PGP can be complicated to learn and because the younger generations prefer instant messengers to email. His argument is that

through the development of popular encryption software and applications, the public can easily protect their communications without having to worry about the logistics (Interview data, 2016).

More radically, with the heavy commercialization of the web alongside aggressive intelligence-gathering programs, using encryption as a tool to communicate in private is more important than ever. Gill has explained that a perfect system of information can be dangerous for democracy, as great social progress can come from "illegal" ideas which need to be explored and shared in secret:

> When you start building a system of perfect or complete information access, that can be really dangerous. When a government has perfect information, at least at a theoretical level it's only a question of resources until they are able to engage in perfect enforcement. And perfect enforcement of the law is terrible for democracy. Almost every single one of us has been a criminal in some way in our lives and even from a very moderate liberal democratic framework, most people would accept that a certain amount of illegality is critical to social change. There is no major movement toward social progress that's ever happened in this country or any country that I can think of that didn't involve a dimension of illegality. You know, the specter of a Big Brother type system, part of what these stories and images in our history highlight are the right to think dangerous ideas- to think illegal ideas, to do the occasional subversive illegal thinking is actually critical to how history changes (Interview data, 2016).

Equally, David Kaye, the U.N's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has come to the conclusion that encryption is not only helpful to journalists, criminals, whistleblowers, and activists, but should be seen as a fundamental human right against digital privacy invasion: "The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality" (Froomkin, 2015). As we have shown, the stakes for supporting strong encryption are high, but the Snowden disclosures beg the following questions: whose responsibility is it to protect the privacy of Internet users? Is it the corporations, who are responsible for opening the door to mass surveillance on the Internet in the

first place? Is it the governments, who have the duty to protect the privacy of its people and uphold its constitutions while managing threats against national security? Or, is it the individuals, whose marginalized populations are doomed to get left behind while the technologically literate have greater access to privacy? As there are no easy answers to these questions, each of my interviewees offered a slightly different take on them. While Vitaliev argues that educating the public about digital privacy is key, Gill has added that software developers should recognize their role in a highly political battle where illegal ideas are conducive to social progress. Thaler focuses on pushing forward with encrypted messenger applications to outshine email, and Dr. Light looks for ways that telecom companies can work with the law to protect their customers' privacy (Interview data, 2016). He has also created a portable Snowden archive for people to browse through the documents without the fear of being targeted for extra surveillance by intelligence and law enforcement.

In summary, encrypting digital content is the best way to secure data in transit from one device to another. Although metadata such as who is contacting whom cannot be encrypted, it is still a strong online privacy tool. Since the mathematics behind strong encryption became public, the upheaval of government initiatives to limit or outlaw encryption software during the first crypto war was a significant success for Internet activists in the 90s. A wide variety of factors are involved in the future of the internet. In short, providing the governments with backdoors to encryption protocol undermines the whole point; people should be free to express and explore their human development online without worrying about interference from warrantless state intervention or corporate actors prying into their personal business. For the time being, encryption is the best risk management solution to evade state surveillance even if government reform comes slowly or not at all.

[1] USA FREEDOM stands for "uniting and strengthening America by fulfilling rights and ending eavesdropping, dragnet-collection and online monitoring act"

[2] History of the First Crypto War, Bruce Schneier's blog https://www.schneier.com/blog/archives/2015/06/history_of_the_.html

[3] A Message To Our Customers, Apple v. FBI case: https://www.apple.com/customer-letter/

[4] However, through a program called EGOTISTICAL GIRAFFE, the NSA has been known to target TOR users for extra surveillance by inserting vulnerabilities in their computers. See http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document

# Chapter Five

## Social Change

If we have learned anything about the digital communications technologies that have been developed over the past couple of decades, it's that they are used in conflicting ways, supporting political activism and organization on the one hand while simultaneously facilitating corporate and government surveillance on the other. In either case, the potential of Big Data holds exciting prospects for research in the social sciences. As the field of sociology has struggled with new methodologies and ethical concerns of studying the social world(s) of the internet, corporate and government bodies have wasted no time capitalizing on user-generated content perpetuated by the sharing culture of Web 2.0 applications. The internet and its accessories can be considered a double-edged sword; news about the Snowden leaks have been shared through the very same online platforms that are under scrutiny for their secret involvement with intelligence agencies. As academic work (i.e. Deleuze, 1992) has traditionally conceptualized digital privacy with highly theoretical language and discourse, this research has outlined the development of Snowden's story and some of the key documents subsequently published by *The Guardian* and other media outlets from a more accessible level of writing and understanding. With hopes to contribute to a movement towards social progress regarding internet surveillance and privacy, this paper has explored critiques of dragnet surveillance programs, telephony metadata programs, webcam spying, encryption compromising, wiretapping, boomerang routing, outdated legal justifications, issues with government transparency and serious accountability. Journalistic reporting on the Snowden documents in conjuncture with the expertise of four interview respondents has greatly informed this work. Because the Snowden story is relatively new, this research contributes to the new wave

of early scholarly work surrounding post 9/11 surveillance in the Western world. Finally, this chapter explores the future of digital privacy alongside the uneven distribution of risk associated with surveillance techniques and technological advances.

## The Future of Digital Privacy

The Snowden documents help to unpack some of the NSA's questionable interpretations of the law. To legally justify dragnet surveillance programs, the definitions of words like "relevant" and "incidental" have been constructed in interesting ways. Since 9/11, the NSA collected all American telephone metadata "relevant" to an investigation under the Patriot Act. Though the Patriot Act was never supposed to enable mass surveillance, the NSA argued that since they could not know what was "relevant" without seeing it first, they need to collect as much data as possible without a search warrant in order figure out what was "relevant" later:

> The Department of Justice's national security lawyers combed through the law looking for loopholes. Even though the law was intended to facilitate targeted surveillance, they decided it could be stretched to authorize mass surveillance…they were able to convince a judge that everything was 'relevant' to an investigation. This was a new interpretation of the word 'relevant; one that doesn't even pass the sniff test. If 'relevant' doesn't restrict collection because everything is relevant, then why was the word put into the law in the first place? Even Congressman Jim Sensenbrenner, the person who wrote the USA PATRIOT Act, was surprised when he learned that the NSA used it as a legal justification for collecting data on Americans. 'It's like scooping up the entire ocean to catch a fish', he said (Schneier, 2015: 124)

In another example, even though Section 702 of the FISA amendments doesn't explicitly authorize mass surveillance, the NSA interprets the law in ways that allow it to collect content and metadata on hundreds of millions of people under similar reasoning. The law is meant to facilitate eavesdropping on foreign targets if their communications pass-through US territory. Collecting warrantless intelligence on American citizens is illegal, but any information collected on

Americans while sweeping up foreign communications is considered "incidental" to be used as fair game for evidence for other crimes after it had been collected. Bruce Schneier agues that this is the same logic as having the police search every home in America while investigating someone from Bulgaria and claiming that "none of the other searches counted because they hadn't found anything, and what they found was admissible as evidence because it was 'incidental' to the search for the Bulgarian" (Schneier 2015: 125).

In terms of investigating what changes that have been made since the initial release of the Snowden documents, we can point to some micro movement towards a digital-privacy friendly future. Fierce political discussions following the Snowden documents resulted in the USA Freedom Act replacing the Patriot Act[1] with several modifications in 2015. After *ACLU v Clapper (*2015), the court ruled in favour of the American Civil Liberties Union on appeal: "the court found that [Patriot Act's] Section 215's authorization of the collection of business records that are 'relevant to an authorized investigation' could not be read to include the dragnet collection of telephone records" (Greene, 2015). Instead of automatically collecting all American telephone metadata from companies like Verizon and AT&T, the USA Freedom Act now requires intelligence agencies to acquire a warrant for specific phone records from the FISA court before obtaining the data. Although this can be considered a win for privacy advocates, DNI James Clapper boasted about being pleasantly surprised that since the Snowden leaks, this was the only program the NSA had to revoke, and that they hadn't lost access to the data since they can still get it from the phone companies (Froomkin, 2015).

In the last couple of years, we have learned much about the NSA's changing relationship with companies like Google, Facebook, Microsoft, and AT&T. Recently placed under public

scrutiny, the head honchos of the tech world have attempted to distance themselves from intelligence agencies by lobbying to influence Congress or flat out refusing to cooperate with FBI investigations. In an open letter to the Senate, ten major internet companies joined forces to fight towards limiting government data collection and adding more transparency and accountability protocol under the USA Freedom Act in 2015[2]. CEO Tim Cook has publicly outlined Apple's policies in support of encryption[3] through their legal battle with the FBI in December of 2015. Their own messaging system, iMessage, operates under end-to-end encryption to protect user communications. Other encrypted call and message applications developed by non-profits like Open Whisper Systems (OWS) are becoming widely used. After Snowden's releases, many major websites have adopted HTTPS (Hyper Text Transfer Protocol Secure)[4], which is protocol that encrypts information traveling between servers and websites. One of the biggest results of the Snowden disclosures involved Gmail implementing HTTPS to secure all emails flowing between their data centers and their servers[5] (Vitaliev, Interview Data, 2016). HTTPS is what allows for secure browsing and banking to take place online; without it, the full content of communications, websites browsed and search terms typed are viewable to anyone on the network (Barrett, 2016). Pew research has shown that corporations aren't the only ones changing their habits, as 34% of Americans aware of the Snowden documents have since taken steps to secure their online communications (Rainie & Madden, 2015).

In the related sector of state law enforcement and technology, small changes are taking place as well. In 2014, the Supreme Court of the United States sided with the ACLU and the Electronic Privacy Information Center (EPIC) in *Riley v. California*[6], marking unwarranted cellphone searches of people who have been arrested illegal in California (Swaine, 2014). In Canada, a similar Supreme Court ruling unfolded in *R. v. Fearon* (2014) where Canadian cell

phones may only be searched during a lawful arrest to find recent evidence pertaining to the charges at hand. Further, the police must appropriately document such searches, and are limited to recent cellphone activity pertaining to the investigation. In discussing the legality of police cellphone access, Canadian Justice Karakatsanis likens today's cellphones to keys to personal lives, thus arguing that police should have limited accessibility to them:

> The fact that a suspect may be carrying their house key at the time they are arrested does not justify the police using that key to enter the suspect's home. In the same way, seizing the key to the user's digital life should not justify a wholesale intrusion into that realm (*R. v. Fearon*, 2014: para 132).

In many ways, efforts towards private digital networks have barely scratched the surface. Without whistleblowers and Freedom of Information Acts, it is near impossible to tell what surveillance programs are still active and what new ones have been initiated. From what we do know, however, the reality is grim. Initiatives to keep national data secured within borders are undermined by international trade deals that operate outside of the scope of national law such as the TPP. Any initiatives to protect sensitive information (such as health or income data) from crossing borders will be powerless under the new agreement which aims to capitalize on data mining (Geist, 2015a). Within the borders, the extensive data collection capabilities of Canadian intelligence have only expanded under Bill C51. With the technology we have today, the abuse of authority is all too easy. In a 2016 interview with *Vice*, Snowden showed how the cameras and microphones in smartphones can easily be hacked and manipulated to see and hear anything the user sees or hears, and there is no way to tell whether a phone has been compromised. When asked whether the NSA, FBI and CIA can access the contents of laptops, iPads and cellphones, Snowden replied:

> Yes…absolutely…As long as they can dedicate people, money and time to the target, they can get in…Everything in your contacts list, every SMS message that you use, every place that it's ever been, where the phone is physically located…even if you've got GPS disabled because they can see which wireless access points are near you. Every part of private life today is found on someone's phone. We used to say a man's home is his castle, today, a man's phone is his castle. (*Vice*, 2016: 4:01-4:33)

In the *Vice* interview, Snowden goes on to argue that part of the reason people seem uninterested in surveillance programs is because they were implemented in secret. If the Canadian or American government suddenly announced that every home in the country were to be equipped with cameras or microphones to monitor every conversation, "people would be up in arms about it", (*Vice*, 2016:4:48, 4:53) he says. Cellphone and laptop users have willingly purchased the digital devices of their own surveillance, carrying them everywhere. The question is not whether authorities can exploit handheld devices and personal computers, the question is whether they will. Snowden's essay in *The Intercept* shows that heavy spying technologies start in the foreign surveillance realm and slowly inch their way into civilian spy programs at home. If internet users fail to fight for secure networks, government transparency and policy reform, extensive unwarranted surveillance tactics will only continue to gain momentum through new technologies such as drone monitoring:

> Take, for instance, the holy grail of drone persistence, a capability that the US has been pursuing forever. The goal is to deploy solar-powered drones that can loiter in the air for weeks without coming down. Once you can do that, and you put any typical signals-collection device on the bottom of it to monitor, unblinkingly, the emanations of, for example, the different network addresses of every laptop, phone and iPod, you know not just where a particular device is in what city, but you know what apartment each device lives in, where it goes at any particular time, and by what route (Snowden, 2016).

As exploiting "smart" devices such as wearable tech[7] and predictive analytics are the next big surveillance trends (Zuboff, 2015), patterns in location data can be easily analyzed to accurately guess where a tracked cellphone user will be the next day: "researchers were able to use

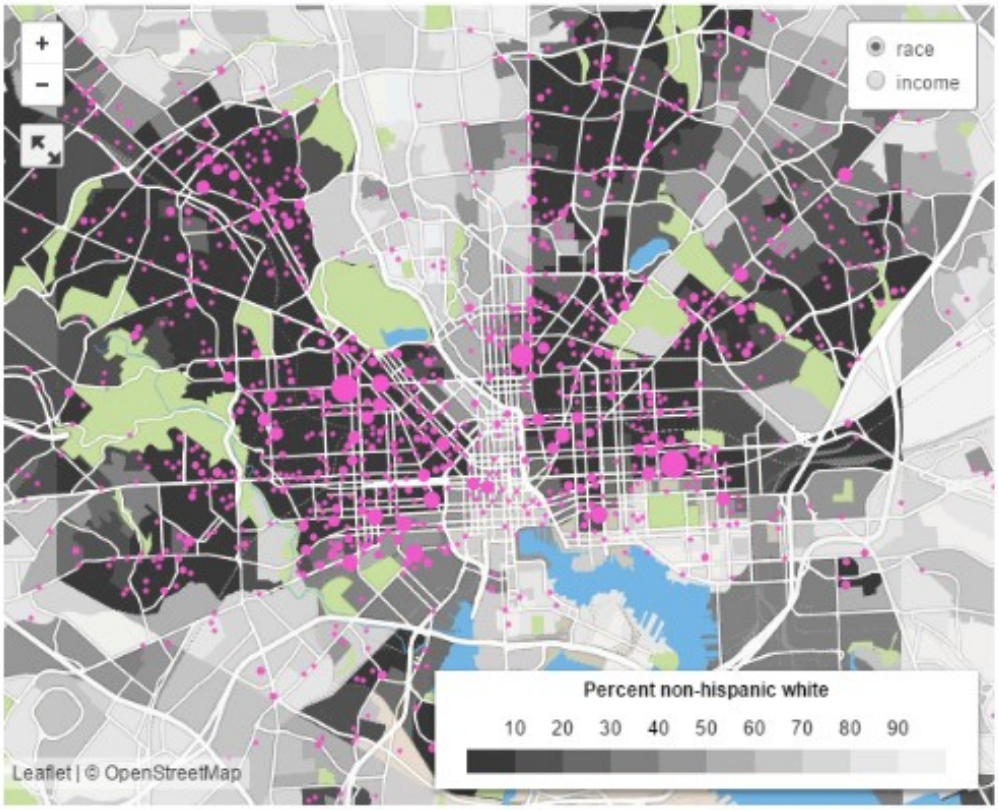
this [cellphone location] data to predict where people would be 24 hours later, to within 20 meters" (Schneier, 2015:7). Data bodies tell stories about individual identities, their communications, their whereabouts, and their innermost thoughts and desires. The right to encryption and the right to be forgotten represent two crucial privacy debates of our time. As we have seen, once surveillance programs and mechanisms are put into place, they are very hard to revoke. Following Zuboff's third law, in the absence of serious public opposition and activism, surveillance society will only continue to move further towards social control and behavioural manipulation through technological means (2013).

## Uneven Distributions of Risk

### Social Movements and Surveillance

Snowden's prophecy on drone surveillance is not as far-fetched as it may sound; new technologies can be detrimental to the organization of social movements. We have already seen examples of mass communications being swept up by the FBI flying aircrafts over major US cities during the Black Lives Matter protests (Stanley, 2016; *Vice*, 2016). This type of surveillance is conducted without warrants, and is often used to criminalize political dissidence. As explained by Snowden: "The FBI has a specific aviation unit that's flying around cities, and frequently they're monitoring protesters rather than violent criminals. In Baltimore, during the Black Lives Matter protests, the FBI was flying surveillance over the protesters" (*Vice*, 2016: 9:40-9:54). Collecting data on every single person with a cellphone involved in a protest is a scare tactic that infringes on basic civil liberties such as freedom of association, the right to peaceful protest, the right against unreasonable search and seizure, and the right to free speech. Signal tracking devices such as Stingray IMSI-catchers have become more popular with North American law enforcement in recent years. These devices work by mimicking cellphone towers to intercept signals and locate

devices; they can also be used to intercept cellphone content (Lynch, 2016b). To date, law enforcement has been very secretive about IMSI use, but through FOIA requests, we can deduct that cellphone tracking technology has been used to over-police low income and minority groups, while avoiding targeting affluent white areas in the US (Joseph, 2016).




Stingray use in Baltimore, Maryland. (Frankie Dintino/CityLab)

The CityLab research above features a modern example of a well-documented pattern of discrimination bias in surveillance culture. In Baltimore, where African-American communities are targeted with Stingray technology 90% of the time, and low income areas were targeted 70% of the time (Joseph, 2016). The circles indicate the frequency distribution of Stingray usage. When using this data to compare four different cities with similar crime rates in Baltimore (two predominantly white areas, Hampden and Woodbury, and two predominantly African-American

areas, Resevoir Hill and Penn North) with similar crime rate levels, the Stingray catchers were overwhelmingly used to spy on low income non-white neighborhoods. The same research conducted in Milwaukee and Tallahassee resulted in similar findings of over-policing and surveillance in communities of color (Joseph, 2016). The Civil Rights Coalition has filed a case with the FCC to dispute the legality of using these devices as well as the racial profiling apparently associated with their use (Lynch, 2016b). Snowden warns that cellphone location data can hypothetically place people at a scene of a crime they did not commit:

> Let's imagine a thought experiment, I know everything that you've done for 30 days. I have all your metadata. I know where you're at, I know how fast you were travelling down the highway, I know which toll roads you went to. At the end of 30 days, I accuse you of a crime that you didn't commit. Do you think you can beat that charge? (ViceNews, 2016 1:08 – 1: 24)

While the prospect of listing pre-suspects is attractive to law enforcement, Jennifer Lynch of the EFF has shown that predictive policing algorithms are most often being used to track economically vulnerable populations who are already under extra surveillance by law enforcement, such as low-income communities (2016a). Mills has also argued that crime prediction programs are operating with a low level of accuracy in their early stages of development (2015). In *When Biometrics Fail*, Magnet has shown that biometric technology used by governments to track immigrants, prisoners, and other marginalized members of the population most often malfunction when being used to evaluate non-white bodies, women, and people with disabilities, suggesting that discrimination bias is programmed into technology itself (Magnet, 2011). In another instance, a study with a sample size of 7000 people concluded that a crime prediction program frequently mislabelled black males as "risky" significantly more often than white men (Anguin et. al, 2015). Even if predictive policing worked effectively, As Gill explained in our interview, perfect enforcement of the law is not always healthy for democratic progress:

> For example, there was a time where providing an abortion was a criminal offense. There was a time in many US states where interracial marriage was a criminal offense. These things are of course no longer criminal. Yet queer rights, women's access to reproductive healthcare, and the end of racial segregation did not come about because people in power spontaneously changed their minds. They happened as a result of long and difficult campaigns, vast public education efforts, relentless advocacy, costly lawsuits, and yes, sometimes civil disobedience. I think we have to look at history with our eyes wide open, and recognize that simply because something is "law" that does not necessarily make it moral, or right. The law is a living, breathing thing. It is imperfect, and part of the pursuit of justice is the search for something more perfect, more just. So we can only hope that a hundred years from now, our laws and institutions of justice are more fair, equitable, just and principled than they are today. And we can only hope that people are willing to fight for that. Unlimited, unchecked and unaccountable systems of surveillance ("collecting it all") open the door to a more "perfect" enforcement of the law. And that makes social change very difficult — not only because it frustrates the ability of individuals to engage in what we might think of today as "civil disobedience," but because the law itself is a moving target, and what we consider today to be perfectly -legal- activity can quickly become illegal depending on changing circumstances. For example, during the Toronto G20 the Ontario government passed a law that gave police extraordinary search and arrest powers[1] and during the Quebec student strikes in 2012 the Quebec government passed a rule banning unapproved assemblies of 50 or more people at a time[1] Though both of these laws were almost certainly unconstitutional and eventually repealed, a legal challenge can take years and thousands of dollars. In the short term, they turned innocent people engaged in constitutionally protected speech and assembly into suspects and criminals (Gill, Interview data, 2016).

Throughout history, marginalized and activist groups are disproportionately targeted by the state by surveillance programs (Lynch, 2012). From 1956-1971, the FBI's COINTELPRO (Counter Intelligence Program) monitored, infiltrated, discredited and harassed supporters of the Communist Party, the Black Panther Party and non-violent activists involved with anti-war efforts and the civil rights movement. Following an activist break-in to FBI offices in 1971 where over one thousand top-secret files were stolen and distributed to the media, the FBI was sued for not handing over further information about COINTELPRO via FOIA requests during the Nixon administration. Once the COINTELPRO documents were finally released, the first Congressional investigation of U.S. intelligence agencies (the Church Committee) found disturbing details about illegal practices of the FBI. For example, the FBI had been secretly infiltrating women's liberation

groups that had nothing to do with crime or violence, they had been posing as university students to identify socially radical students and professors, and they had even sent anonymous threatening letters to Dr. Martin Luther King in an effort to get him to end his own life (Hamilton, 2014). Later, many of the surveillance tactics involved in this program were found illegal by the Senate's Church Committee and COINTELPRO was revoked (Kayyali, 2014). Consequently, 500 FBI offices were shut down and intelligence agencies such as the NSA and the FBI were placed under tighter regulations and oversight boards (Hamilton, 2014). Then, after 9/11, many of these legal precautions to avoid the abuse of power were ignored, as questionable interpretations of the Patriot Act and section 702 of the FISA amendment helped intelligence agencies gain sweeping surveillance powers over entire populations. According to Matthew Jones, numerous provisions of the legislation needed to support these programs were drafted and ready to be signed long before 9/11, as the intelligence community and law enforcement communities were just waiting for something nationally catastrophic to happen to justify their approval (Jones, 2016).

More recently, the NYPD spied on the Occupy Movement by infiltrating student groups, ethnic communities and spying on mosques: "many of these operations were conducted with the help of the CIA, which is prohibited by law from spying on Americans" (Schneier, 2015:76). The Black Lives Matter movement has resulted in heated political debates surrounding the intersectionality of race and class in relation to law enforcement. In the US, social media users expressing disdain for the police have been arrested and charged with disorderly conduct or public intimidation (LaChance, 2016). An internal document from the Customs and Border Protection Bureau drafted in 2016 suggests that the US border patrol may soon be requesting visitors to the US to disclose their social media contact information and links before being admitted into the country[8]. State initiatives to monitor and limit speech on social media channels can lead to

undermining values of freedom of expression. Thus, censorship by fear of being monitored or arrested may intimidate users into silencing their views on political issues on the internet. As we have seen, intelligence agencies tend to interpret the law in ways that favor their own ends, making it possible to collect information on anyone with "radical" political views, whether or not the targeted individuals are violent or criminal. Digital technologies such as algorithmic crime prediction programs or IMSI catchers can be used to target political activists and marginalized populations under the guise of national security and unbiased law enforcement.

## Surveillance Capitalism

As we have shown, there are two major reasons internet users are exploited for their data; profit and intelligence gathering (Wasserman, 2015:115). State-run data collection programs were performed largely in secret before the Snowden disclosures; they never had a chance to be debated by an informed democratic public before being set into motion. Surveillance capitalism, according to Zuboff, thrives off invading the privacy of others, yet builds the highest walls around its own organizations and practices. As Zuboff argues, although internet users are both the generators and the objects of Big Data, digital rights are an inconvenient afterthought in the minds of both intelligence agencies and corporations: "While 'Big Data' may be set to other uses, those do not erase its origins in an extractive project founded on formal indifference to the populations that comprise both its data sources and its ultimate targets" (Zuboff, 2015:76). Surveillance capitalism tactics are even more extensive than intelligence agency programs: "While the world is riveted by the showdown between Apple and the FBI, the truth is that the surveillance capabilities being developed by surveillance capitalists are the envy of every state security agency" (Zuboff, 2016:1). To illuminate what the future of Big Data holds for consumers, Zuboff points to car insurance

companies relying on "automotive telematics" to hike rates or even shut down car engines in real-time. Data collection about driving habits also allows the possibility for auto insurance companies to mimic Google's business model by selling information about immediate realities to third-parties:

> The game is selling access to the real-time flow of your daily life –your reality—in order to directly influence and modify your behavior for profit. This is the gateway to a new universe of monetization opportunities: restaurants who want to be your destination. Service vendors who want to fix your brake pads. Shops who will lure you like the fabled Sirens (Zuboff, 2016:2).

Widespread voluntary participation on social media platforms and the constant use of handheld devices only amplify exploitative relations between technology users and the agents of surveillance. As the logic of capitalist accumulation seeps into many subsections of society (Fuchs, 2013), the NSA and Google both fight to collect as much data on the population as they can for the sake of political and financial power. Chief data scientists of Silicon Valley admit the end goal of predictive analytics is to collect as much data as possible to alter or influence consumer behaviour, which Zuboff also explains by applying the logic of capitalist accumulation to data mining projects as a means of securing corporate power and social control. Understanding mass surveillance under this framework is a helpful starting point for unraveling motivations behind corporate and government behaviour where users are subsequently alienated from their own unpaid activities while ringing in massive profits for corporations. In some cases, corporations can even double up on profit from users, first from subscriptions and second from data-collection based advertisements:

> Verizon's acquisitions of AOL and Yahoo are both aimed at monetizing Internet usage beyond the straightforward sale of broadband access. With greater insights into customer behavior, the company could market additional services or content to its wireless subscribers as part of a bundle, policy analysts say. That arrangement could allow

> Verizon to effectively earn money twice from the same subscriber — once for the data plan, and then again when the customer consumes Verizon-affiliated content (Fung & Timberg, 2016).

This same data on location, finances, health, and browsing history may also be used against them in the form of racial, class-based or ideological discrimination from a wide variety of institutions by way of third-parties (Zuboff, 2015). While the internet can be used as an astonishing tool for human connection, social progress and learning, the panoptic effect of constant surveillance limits the potential for civil disobedience and organization as well as intellectual development through exploration. As a potential solution to unwarranted corporate surveillance, Tim Berners-Lee has publicly responded to the prospect of unwarranted corporate data collection by proposing a change in internet protocol that involved users gaining control over their own data, giving them the option to sell their data to companies if they so choose but otherwise keeping it private (Curtis, 2014). In October 2016, the FCC (Federal Communications Commission) passed legislation that limits user data collection and sharing capabilities of ISPs (Internet Service Providers). Tom Wheeler, chairman of the FCC has been quoted saying: "it is the consumers' information, it should be the consumers' choice" (Fung & Timberg, 2016). Some say these new rules will only give more of an advantage to websites (such as Google and Facebook) who engage in the same activity (Fung & Timberg, 2016). As a response, FCC commissioner Ajit Pai FCC has suggested individual companies should be next on the FCC's list of priorities: "If the FCC truly believes that these new rules are necessary to protect consumer privacy, then the government now must move forward to ensure uniform regulation of all companies in the Internet ecosystem at the new baseline the FCC has set" (Fung & Timberg, 2016). Social change in the digital world needs to come from all levels of engagement: government regulation, corporate responsibility, software development and user vigilance.

Now, although Edward Snowden has succeeded in bringing a general awareness of civilian spy programs into the public consciousness through online media, serious change in this arena has been slow. The ideological opposition to mass surveillance simply isn't strong enough to resist the incessant force of the military industrial complex of the US and its Five-Eye partners. Geist has critiqued Canadians as being particularly silent on this issue, referring to the Canadian response as "muted at best" (2016). In the U.S., little change has been made to intelligence and law enforcement protocol since Snowden. However, new ISP regulations brought forward by the FCC hint towards progress in the corporate sector, and organizations like the ACLU and Privacy International have been using the Snowden documents to build legal cases against NSA programs. While current online networks have government surveillance systems interlaced into the backbone of the internet itself (Wasserman, 2015), a global digital rights reform is undeniably needed if John Perry Barlow and Tim Berners Lee's dreams of cyber-optimism are to ever come to fruition.

## Conclusion

Throughout this thesis, we have discussed the ways in which internet use contributes to potentially exploitative surveillance practices. First, unpaid internet users generate immense capital for social media websites and popular search engines such as Google, which in turn generates value for third party advertisers. Then, the data generated by internet users is further collected for policing and intelligence purposes. Data trails can work to influence insurance rates, employment opportunities, bank loans, and even criminal cases. Justified under the guise of national security in a post-9/11 world, civil liberties are undermined by invasive surveillance programs in the absence of public awareness. Snowden has argued that "collecting the haystack" has only proven less effective than traditional means of targeted surveillance in terms of stopping

crime and fighting terrorism. In addition, unwarranted surveillance programs have been subject to power abuse and questionable ethics. Aside from spying on civilian webcam activity through OPTIC NERVE, a program codenamed LOVEINT has allowed some NSA employees to use national security databases to secretly monitor their intimate partners (Ackerman & Ball, 2014; Schneier 2015:76). This information presented in these documents is disturbing and out-of-sync with democratic values such as the right to privacy and freedom of speech. For these reasons, both academia and journalism should work together to raise awareness on serious issues such as these. In this work, I have aimed to make this information accessible, swaying away from high-level theoretical arguments and specialized language that convolute the pressing issues at hand. With the belief that political sociology should be written in such a way that encourages citizen engagement, participation, and hands-on learning, I hope to have contributed a unique project to the new wave of work on surveillance and society.

If the governments of liberal democracies remain neither accountable nor transparent to the public, the time has come to recognize the need for guerilla accountability (Whitaker, 2015). The secrecy behind ubiquitous mass surveillance makes it important for whistleblowers like Edward Snowden to engage the public in meaningful debates about what sorts of governments citizens want to decide to support or reject. For citizens of a democracy to be able to vote for policies and representatives they support, they need access to information about what their own governments are doing and promising. In the absence of official disclosure about programs that affect us all, whistleblowers and journalists need access to appropriate legal channels to safely leak information to the public. They should be able to do so in a way that minimizes harm to national security while respecting the public's right to know. To ensure that the prospect of whistleblowing itself is not abused, leakers need access to fair trails that allow them to explain their actions to a

jury of their peers, which is currently unfeasible under the Espionage Act. As encryption remains the best method for securing private communications, software developers and cryptographers might reconsider their roles as political figures in the dawning of the Information Age. Equally, internet users should recognize their stake in the fight over their own futures. As Snowden insists: "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say"[9] (2015). If the future of democratic society is to be compatible with basic civil liberties such as freedom of speech and the right to privacy, the time to protect them is now.

---

[1] Section 215 of the Patriot Act, the post 9/11 legislation that allowed for NSA to collect all metadata on cellphone calls within the United States has since been revoked and replaced by the USA Freedom Act which doesn't permit this program.

[2] Global Government Surveillance Reform: An Open Letter to the Senate https://www.reformgovernmentsurveillance.com/

[3] Tim Cook's customer letter in support of encryption http://www.apple.com/customer-letter/

[4] Research suggests that HTTPS use has more than doubled in the past few years https://pardonsnowden.org/news/snowden-effect-on-tech

[5] Now Gmail Encrypts Every Email. Google CEO Larry Page was publicly disappointed in Snowden disclosures: "For me, it's tremendously disappointing that the government sort of secretly did all these things and didn't tell us. I don't think we can have a democracy if we're having to protect you and our users from the government for stuff that we never had a conversation about." http://www.slate.com/blogs/future_tense/2014/03/21/gmail_will_now_encrypt_all_of_the_traffic_between_google_servers_to_make.html

[6] Supreme Court decision, *Riley v. California* https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

[7] Biosensors to Monitor US Students Attentiveness http://www.reuters.com/article/us-usa-education-gates-idUSBRE85C17Z20120613

[8] Regulations.gov Agency Information Collection Activities: Arrival and Departure Record (Forms I–94 and I–94W) and Electronic System for Travel Authorization

https://www.regulations.gov/document?D=USCBP-2007-0102-0016

[9] Nothing to hide quote, Snowden on Ask Me Anything, Reddit https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/crglgh2/

## Appendix of NSA Programs

Stellar Wind: Bulk metadata collection of American phone calls and internet traffic/ no warrant needed/FISA/Constitution does not apply because Americans should have no reasonable expectation of privacy (until 2011). (Mills, 2015: 210-217).

PRISM: "Direct content extraction" from Microsoft, Google, Yahoo, Skype, Facebook, Youtube, AOL and Paltalk servers: "NSA can collect shared content ex. Emails, chats, videos, photos, stored data, voice over Internet protocol, file transfers, videoconferencing, log ins and social networking details – any individual or American"/ SEC 702 FISA- Constitution does not apply/no need for court order or "authorization from the service providers" (Mills, 2015: 210-217).

UPSTREAM: NSA/GCHQ wiretapping underwater cables: "cable communications collected include phone call recordings, email messages, Internet history and Facebook content… Data is preserved for 3 days and metadata is stored for thirty days… Appears to be no distinction between innocent individuals and targeted suspects." Section 702/FISA/Constitution does not apply because "the actions take place outside of the United States" (Mills, 2015: 210-217).

Cell Phone Records (RAGTIME and MARINA programs): "Court order requiring the provision of electronic copies of "telephony metadata" in bulk to the NSA by Verizon. The data is then stored in a NSA database." Call location/length/ session identifying information placed by US citizens… without any evidence of wrongdoing by the caller of the person being called. The NSA can then search through these results within three hops of a preapproved seed number connected to a foreign terrorist organization…NSA would supposedly need an additional warrant to access the data". Section 215 Patriot Act Constitution does not apply because "(1) there is no reasonable expectation of privacy for Americans and (2) foreign targets do not receive constitutional protections" (Mills, 2015: 210-217).

CO-TRAVELLER: "NSA taps into global cable network connections (i.e. telephony links) and intercepts data pertaining to the location of cell phones through cellular networks, GPS, Wi-Fi and triangulation" used to track location data, no evidence of wrongdoing required. "(1) there is no reasonable expectation of privacy for Americans and (2) foreign targets do not receive constitutional protections" (Mills, 2015: 210-217).

MUSCULAR: "Extraction of unencrypted data in bulk from Google and Yahoo's overseas fiber optic cables by hacking into their internal networks, supposedly without the authorization of the ISPs. After being collected, the data is then filtered and sorted… This allows the NSA to copy data and content in real time without the knowledge or permission of the providers" "Attorney General approved processes" and "(1) there is no reasonable expectation of privacy for Americans and (2) foreign targets do not receive constitutional protections" (Mills, 2015: 210-217).

XKEYSCORE: Search engine for all civilian spy program databases on over 700 servers: "Allows the NSA to retrospectively search through their bulk data collection for any type of information

(e.g., a telephone number, or an individuals Google searches) without a warrant". "Legal justification not known" (Mills, 2015: 210-217).

SIGINT: Used to weaken encryption standards that protect data "Digital insertion of vulnerabilities into encryption systems, IT networks and Tor". "Legal justification not known" (Mills, 2015: 210-217).

National Security Letters: "After an ISP or phone company receives an NSL, they are required to submit user profile information to the FBI. While the law supposedly limits the FBI from content such as e-mail or text messages, the companies are usually under a gag order and cannot alert their users that this information has been shared." Legally justified by I8 USC and 2709—expanded by Sec. 505 Patriot Act. USCA Second Circuit held 2709 and 3511 (b) unconstitutional based on their lack of juridical oversight for the nondisclosure requirements" (Mills, 2015: 210-217).

LEVITATION: Untargeted CSE monitoring every upload and download made in Canada, less than 1% of interest. (Geist, 2015).

Optic Nerve: GCHQ and NSA program used to collect live images and videos from unsuspecting webcam users in their homes (Ackerman & Ball, 2014).

**Works Cited**


Abell, J. (2015). Open Letter to Parliament: Amend C-51 or kill it. *National Post*. Retrieved from: http://news.nationalpost.com/full-comment/open-letter-to-parliament-amend-c-51-or-kill-it

ACLU v. Clapper (2013, September 4). ACLU v. Clapper Amicus Brief. *EFF*. (https://www.eff.org/document/aclu-v-clapper-amicus-brief

Ackerman S., Ball, J. (2014, February 28). Optic Nerve: millions of Yahoo webcam images intercepted by the GCHQ. *The Guardian*. Retrieved from: http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

American Civil Liberties Union (ACLU). (2015, October 9). ACLU v. Clapper, Challenge to NSA Mass Call-Tracking Program. *American Civil Liberties Union.* Retrieved from: https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program

Andrejevic, M. (2012). Exploitation in the Data Mine. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media.* Routledge. New York.

Andrejevic, M. (2013). Alienation's Returns. *Critique, Social Media and the Information Society*. Edited by Christian Fuchs and Marisol Sandoval. Routledge, England.

Angwin, J., Larson, J., Mattu, S., Kirchner, L. (2016, May 23) Machine Bias. *ProPublica*. United States. Retrieved from: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

AOL, Apple, Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, Twitter, Yahoo (2015). An Open Letter to Washington. *Reform Government Surveillance.* https://www.reformgovernmentsurveillance.com/, retrieved November 13, 2015.

Assange, J. (2014). *When Google Met WikiLeaks*. OR Books. New York. United States.

Associated Press, (October 8, 2013). Brazil Accuses Canada of Spying after NSA leaks. *The Guardian.* Retrieved from: https://www.theguardian.com/world/2013/oct/08/brazil-accuses-canada-spying-nsa-leaks

Ball, J. (2013, September 30). NSA stores metadata on millions for up to one year, secret files show. *The Guardian*. Retrieved from: https://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

Ball, J. (2013b, October 25). NSA monitored calls of over 35 world leaders after US official handed over contacts. *The Guardian.* Retrieved from: https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

Ball, J., Greenwald, G., Schneier, B. (2013, October 4). NSA and GCHQ target TOR network that protects anonymity of web users. *The Guardian.* Retrieved from: *http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption*

Ball, J., Hopkins, N. (2013, December 20). GCHQ and NSA targeted charities, Germans, Isreali PM and EU chief. *The Guardian*. Retrieved from http://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner

Barlow, P., J. (1996, February 8). A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation*. Retrieved from: https://www.eff.org/cyberspace-independence

Barrett, B (2016, March 17). Most Top Websites Still Don't Use A Basic Security Feature. *Wired.* Retrieved from: https://www.wired.com/2016/03/https-adoption-google-report/

Beck, U. (2013, August 30). The Digital Freedom Risk, Too Fragile an Acknowledgement. *Open Democracy*. Retrieved from: https://www.opendemocracy.net/can-europe-make-it/ulrich-beck/digital-freedom-risk-too-fragile-acknowledgment

Berners Lee, T., (2014). A Magna Carta for the Web. TED2014. *Ted Talks*. Retrieved from: http://www.ted.com/talks/tim_berners_lee_a_magna_carta_for_the_web?language=en

Blanton, T. (2015). Secrecy, Surveillance and the Snowden Effect. *After Snowden.* Macmillan. United States.

Bradburn, H. (Director). (2015, October 5). *Edward Snowden: Spies and the Law.* [Documentary]. Retrieved from : https://www.youtube.com/watch?v=lkwrQ6p9JAM

Brunton, F., Nissenbaum, H. (2015). *Obfuscation: A User's Guide for Privacy and Protest*. The MIT Press. United States.

Booz Allen Hamilton. (2013). *Booz Allen Statement on Reports of Leaked Information.* [Press Release]. Retrieved from http://www.boozallen.com/media-center/press-releases/2013/06/statement-reports-leaked-information-060913

Castells, M (2009). The Rise of the Network Society: The Information Age: Economy, Society, and Culture. Blackwell Publishing. United States.

Cate, H., F. (2015). Edward Snowden and the NSA, Law, Policy and Politics. *The Snowden Reader*. Indiana University Press. United States.

CBC News (2015, March 4). Edward Snowden says Canadian Spying has Weakest Oversight in the Western World. *CBC News.* [Video File]. Retrieved from: http://www.cbc.ca/news/canada/edward-snowden-says-canadian-spying-has-weakest-oversight-in-western-world-1.2981051

Clarke, R., Morell, M., Stone, G., Sunstein, C., Swire, P. (2013). Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies. Retrieved from: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Cohn, C. (2016, April 21). Secret Court Takes Anotehr Bite Out of the Fourth Amendment. Electronic Frontier Foundation. Retrieved from: https://www.eff.org/deeplinks/2016/04/secret-court-takes-another-bite-out-fourth-amendment

Curtis, S. (2014, October 8). Sir Tim Berners-Lee calls for new model of privacy on the web. *The Telegraph.* Retrieved from: http://www.telegraph.co.uk/technology/internet/11148584/Tim-Berners-Lee-calls-for-new-model-for-privacy-on-the-web.html

Colombia Broadcasting System, Associated Press (2015, October 15). Snowden: I'd go to prison to return to the US. *CBS News*. Retrieved from: http://www.cbsnews.com/news/edward-snowden-i-would-go-to-prison-to-return-to-the-united-states/

Deleuze, G. (1992). Postscript on the Societies of Control. Vol. 59. MIT Press. Cambridge. United States.

Desilver, D. (2014, January 22). Most Young Americans Say Snowden Has Served the Public Interest. *Pew Research*. http://www.pewresearch.org/fact-tank/2014/01/22/most-young-americans-say-snowden-has-served-the-public-interest/

Eubanks, V. (2014, January 15). The American Prospect. *The Rockerfeller Institute of Government*. Retrieved from: http://www.rockinst.org/newsroom/news_stories/2014/2014-01-15-The_American_Prospect.pdf

Farrell, P. (2013, December 2). History of 5-Eyes. *The Guardian*. Retrieved from: https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer

Fidler, D. (2015). *The Snowden Reader*. Indiana University Press. United States.

Foucault, Michel. (1977). *Discipline and Punish: The Birth of the Prison*. Alan Sheridan (trans.). Vintage Books. New York. United States.

Foucault, Michel. (1978). Security, Territory, Population—Lectures at the Collège de France. Graham (trans.). Picador. New York. United States.

Fox, L. (2013, June 10). Sensenbrenner: Data Mining Missed Red Flags in Boston Bombing. *US News & World Report*. Retrieved from: http://www.usnews.com/news/articles/2013/06/10/patriot-act-author-sensenbrenner-data-mining-led-to-missed-signals-in-boston-bombing

Froomkin, D. (2015a, May 28). U.N Report Asserts Encryption as a Human Right in the Digital Age. The Intercept. Retrieved from: *https://theintercept.com/2015/05/28/u-n-report-asserts-encryption-human-right-digital-age/*

Froomkin, D. (2015b, June 2). USA Freedom Act: Small Step for Snowden Reform, Giant Leap for Congress. *The Intercept*. Retrieved from: https://theintercept.com/2015/06/02/one-small-step-toward-post-snowden-surveillance-reform-one-giant-step-congress/

Froomkin, D. (2015c, June 17). Hayden Mocks Extent of Post-Snowden Reform. *The Intercept*. Retrieved from https://theintercept.com/2015/06/17/hayden-mocks-extent-post-snowden-surveillance-reform-2-years-cool/

Fuchs, C. (2013). Political Economy and Surveillance Theory. Critical Sociology Vol 39, 5, 671-687. Sage Publications, Sweden.

Fuchs, C. (2016). *Reading Marx in the Information Age*. Routledge. New York, United States.

Fuchs, C. (2014). WikiLeaks and the Critique of the Political Economy. *Karl Marx and the Political Economy of the Media and Communication.* International Journal of Communication 8. University of Westminster, UK.

Fung, B., Timberg, C. (2016, October 27). The FCC just passed sweeping new rules to protect your online privacy. *Washington Post*. Retrieved from: https://www.washingtonpost.com/news/the-switch/wp/2016/10/27/the-fcc-just-passed-sweeping-new-rules-to-protect-your-online-privacy/?tid=sm_tw

Gallagher, R., Greenwald, G. (2015, January 28). Canada Casts Global Surveillance Dragnet Over File Downloads. *The Intercept*. Retrieved from: https://theintercept.com/2015/01/28/canada-cse-levitation-mass-surveillance/

Gallagher, R., Hager, N. (2016, August 14). In Bungled Spying Operation, NSA Targeted Pro-Democracy Campaigner. *The Intercept*. Retrieved from: https://theintercept.com/2016/08/14/nsa-gcsb-prism-surveillance-fullman-fiji/

Geist, M., (2015a, October 14). How the TPP puts Canadian privacy at risk. *Michael Geist*. Retrieved from: http://www.michaelgeist.ca/2015/10/how-the-tpp-puts-canadian-privacy-at-risk/

Geist M., Wark, W. (2015b). *Law, Privacy and Surveillance in the Post-Snowden Era.* University of Ottawa Press. Canada.

Geist, M., (2015c) Why Watching the Watchers Isn't Enough. *Law, Privacy and Surveillance in the Post-Snowden Era*. University of Ottawa Press. Canada.

Geist, M. (2016, June 3) Security agencies need 'fess up about illegal privacy breaches: Geist. *The Star*. Retrieved from: https://www.thestar.com/business/2016/06/13/security-agencies-need-fess-up-about-illegal-privacy-breaches-geist.html.

Gellman, B. (August 15, 2013). NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds. *The Washington Post*. Retrieved from: https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html

Gellman, B., Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. Retrieved from: www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-usinternet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (accessed 28 May 2015)

Gill, L., Redeker, D., Gasser, U. (2015). Towards Digital Constitutionalism? Mapping Attempts to Craft and Internet Bill of Rights. Berkman Center Research Publication No 2015-15. Retrieved from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2687120

Goetz, J. (Director), Heilbuth, P.,E. (Director). (2015). *Terminal F: Chasing Edward Snowden*. [Documentary]. Denmark. Retrieved from: https://www.youtube.com/watch?v=Nd6qN167wKo

Goldfarb, R. (2015). *After Snowden*. MacMillan. United States.

Greene, D. (2015, May 11) ACLU v. Clapper and the Congress: How The Second Circuit's Decision Affects the Legislative Landscape. *EFF*. Retrieved from:

https://www.eff.org/deeplinks/2015/05/aclu-v-clapper-and-congress-how-second-circuits-decision-affects-legislative

Greenberg, A. (2013, June 20) Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It. *Forbes*. Retrieved from: http://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-can-collect-and-keep-your-encrypted-data-as-long-as-it-takes-to-crack-it/#5468a5a23a28

Greenwald, G. (2014a). *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State(first ed.).* London: Hamish Hamilton.

Greenwald, G. [WGBHForum] (2014b, May 19). Glenn Greenwald and Noam Chomsky discuss Edward Snowden and the NSA. YouTube [Video File]. Retrieved from https://www.youtube.com/watch?v=ktRzyiIK1p8

Greenwald, G. (2015, March 4). The "Snowden is Ready to Come Home" Story. A Case Study in Typical Media Deceit. *The Guardian*. Retrieved from https://theintercept.com/2015/03/04/snowden-wants-come-home-stories-case-study-media-deceit/

Grayson, A. (2013, October 25). Congressional oversight of the NSA is a joke. I should know, I'm in congress. *The Guardian*. Retrieved from: https://www.theguardian.com/commentisfree/2013/oct/25/nsa-no-congress-oversight

Hewitt, S. (2015). Forgotten Surveillance: Covert Human Intelligence Sources in a post 911 world. *Law, Privacy and Surveillance in the Post-Snowden Era*. University of Ottawa Press. Canada.

Hill, K. (2015, September 25). A Q&A with Edward Snowden. *Fusion News*. Retrieved from: http://fusion.net/story/201737/edward-snowden-interview/

Hopkins, N., Ball, J. (2013, December 20). GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief. *The Guardian*. Retrieved from: https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner

Hamilton, H., L. (2015). "From Eternal Vigilance: NSA Surveillance and Effective Oversight of Government Power". *The Snowden Reader*. Indiana University Press. United States.

Hamilton, J. (2014) *1971.*[Documentary]. United States. Retrieved from: documentary (Hamilton, 2014) 1971http://www.imdb.com/title/tt3478510/

Heuvel, K., V., Cohen, F., S. (2014, October 28). Edward Snowden: A 'Nation' Interview. *The Nation.* Retrieved from: http://www.thenation.com/article/snowden-exile-exclusive-interview/

Hardt, M., Negri, A., (2000). *Empire*. United States. Harvard University Press.

Hardt, M., Negri, A. (2009). *Commonwealth*. Belknap Press. United States.

Israel, T. (2015). Foreign Intelligence in an Inter-networked world: Time for a Re-evaluation. *Law Privacy and Surveillance in the Post Snowden Era*. University of Ottawa Press, Canada.

Jones, M. (2016, October.). Great Exploitations: Data Mining, Legal Modernization, and the *NSA*. Paper presented at McGill Univeristy, Montreal.

Joseph, G. (2016, October 18). Racial Disparaties in Police 'Stingray' Surveillance, Mapped. *The Atlantic, Citylab. Retrieved from:* http://www.citylab.com/crime/2016/10/racial-disparities-in-police-stingray-surveillance-mapped/502715/

Kayyali, D. (2014, February 13). The History of Surveillance and the Black Community. *EFF*. Retrieved from: https://www.eff.org/deeplinks/2014/02/history-surveillance-and-black-community

Kovach, B., Rosentiel, T. (2001). *The Elements of Journalism: What Newspeople Should Know and the Public Should Expect.* Crown/Archetype publishing. United States.

LaChance, N. (2016, July 12). After Dallas Shootings, Police Arrest People for Criticizing Cops on Facebook and Twitter. *The Intercept.* Retrieved from: https://theintercept.com/2016/07/12/after-dallas-shootings-police-arrest-people-for-criticizing-cops-on-facebook-and-twitter/

Lynch, J. (2012). From Finger Prints to DNA: Biometric Data Collection in US Immigrant Communities and Beyond. *Immigration Policy Center*. Immigration Policy Council. United States.

Lynch, L. [HackerFiscalia Richard Maok Riano Botina] (2015, April 5). Edward @Snowden: #BigData #PanamaPapers #Security #HumanRights #SFU #Snowden. *YouTube*. [Video File] Retrieved from: https://www.youtube.com/watch?v=e1acfjqPcpA

Lynch, J. (2016, April 24). Is Predictive Policing the Law Enforcement Tactic of the Future? *The Wall Street Journal*. Retrieved from: http://www.wsj.com/articles/is-predictive-policing-the-law-enforcement-tactic-of-the-future-1461550190

Lynch, J (2016b). Civil Rights Coalition files FCC Complaint Against Baltimore Police Department for Illegally Using Stingrays to Disrupt Cellular Communications. *EFF*. Retrieved from: https://www.eff.org/deeplinks/2016/08/civil-liberties-groups-file-fcc-complaint-arguing-baltimore-police-are-illegally

Lyon, D. (2009). Surveillance, Power and Everyday Life. *Oxford Handbook on Information and Communication.* Oxford. New York, United States.

Lyon, D. (2015). The Snowden Stakes: Challenges for Understanding Surveillance Today. *Surveillance and Society*, 13(2), 139-152.

Lyon, D. [Council of Europe] (2016, June 21). "Liquid" surveillance, digital citizenship and new ways of living online. YouTube [Video File]. Retrieved from: https://www.youtube.com/watch?v=lRfyIbC50fA

Lupton, D. (2014, October 19). Digital Risk Society. Retrieved from http://dx.doi.org/10.2139/ssrn.2511717

MacCharles, T. (2007, January 31). Arar payout raises concerns for MPs. *The Star*. Retrieved from:https://www.thestar.com/news/2007/01/31/arar_payout_raises_concerns_for_mps.html

MacAskill, E., Borger, J., Hopkins, N., Davies, N., Ball, J., (2013, June 21). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian*. Retrieved from: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

MacAskill, E. (2015, March 4). What would happen if he went home, pardon or prison? *The Guardian*. Retrieved from: https://www.theguardian.com/us-news/2015/mar/04/edward-snowden-what-would-happen-if-he-went-home-pardon-or-prison

Magnet, A., S. (2011). *When Biometrics Fail: Gender, Race and the Technology of Identity*. Duke University Press. United States.

May, T. (1994). Crypto Anarchy and Virtual Communities. *Nakamoto Institute*. Retrieved from: http://nakamotoinstitute.org/virtual-communities/

McCrum, K. (2015, September 14). Facebook friends with poor credit rating could soon stop you from getting a loan. *Mirror*. United Kingdom. Retrieved from http://www.mirror.co.uk/news/world-news/facebook-friends-poor-credit-rating-6439463

Menn, J (2015, December 31). Exclusive: Microsoft to warn email users of suspected hacking by governments. *Reuters.* San Francisco.

Mills, L. J. (2015). The future of privacy in the surveillance age. *After Snowden: Privacy, Secrecy and Security in the Information Age*. Ronald Goldfarb, editor. USA. St. Martin's Press.

Morozov E. (2011). *The Net Delusion: The Dark Side of Internet Freedom.* PublicAffairs Publishing. United States.

Panetta, A. (2015, April 5). Maher Arar's arrest, torture, almost stopped by CIA, ex-spy says. *CBC News*. *The Canadian Press*. Retrieved from: http://www.cbc.ca/news/canada/maher-arar-s-arrest-torture-almost-stopped-by-cia-ex-spy-says-1.3021759

Pilkington, E. (2015a, September 24). Edward Snowden calls for global push to expand digital privacy laws. *The Guardian*. Retrieved from http://www.theguardian.com/us-news/2015/sep/24/edward-snowden-international-laws-digital-privacy-video

Pilkington, E. (2015b, August 12). Chelsea Manning may face solitary confinement for having Jenner Vanity Fair issue. *The Guardian*. Retrieved from http://www.theguardian.com/us-news/2015/aug/12/chelsea-manning-solitary-confinement-toothpaste-army

Pilkington, E. (2012, March 12). Bradley Manning's treatment was cruel and inhuman, UN torture chief rules. *The Guardian*. Retrieved from http://www.theguardian.com/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un

Pinto, S. (2015). Two Years After Snowden, the State of Surveillance in Canada. *Canadian Journalists for Free Expression.* Retrieved from: http://www.cjfe.org/two_years_after_snowden_the_state_of_surveillance_in_canada

Poitras, L. (Director) 2014. *CITIZENFOUR*. [Documentary]. USA. Germany. UK. Praxis Films.

Rainie, L., Madden, M. (2015, March 26). Americans' Privacy Strategies Post-Snowden. *Pew Research*. Retrieved from http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/

Reitman, R. (2016, June 6). Three Years Later, the Snowden leaks have changed how the world sees NSA surveillance. *Electronic Frontier Foundation*. Retrieved from: https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance

Rushe, D. (2014, September 12). Yahoo $250,000 daily dine over data refusal was set to double 'every week'. *The Guardian.* Retrieved from: https://www.theguardian.com/world/2014/sep/11/yahoo-nsa-lawsuit-documents-fine-user-data-refusal

Rogaway, P. (2015). The Moral Character of Cryptographic Work. Cryptology ePrint Archive, Report 2015/1162. New Zealand

Rowan, D. (2014, March 18). Snowden: Big revelations to come: reporting them is not a crime. *Wired*. Retrieved from http://www.wired.co.uk/news/archive/2014-03/18/snowden-ted

Schmidt, M. (2014, July 20). Racy Photos Were Often Shared At NSA, Snowden says. *The New York Times.* Retrieved from: http://www.nytimes.com/2014/07/21/us/politics/edward-snowden-at-nsa-sexually-explicit-photos-often-shared.html?_r=0

Schneier B. (2014, October 6). iPhone Encryption and the Return of the Crypto Wars. *Schneier on Security.* Retrieved from. www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html

Schneier, B. (2015) *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* United States. W.W. Norton.

Simon, B. (2005). The Return of Panopticism: Supervision, Subjection and the New Surveillance. *Surveillance and Society* (3) 1. P1-20

Stanley, J. (2016, August 24). Baltimore Police Secretly Running Aerial Mass-Surveillance Eye in the Sky. *ACLU.* Retrieved from: https://www.aclu.org/blog/free-future/baltimore-police-secretly-running-aerial-mass-surveillance-eye-sky

Sunde, P. (December 11, 2015) I have given up. *Vice Motherboard.* Canada.

Swire, P., Ahmad, K. (2011). 'Going Dark' Versus a Golden Age of Surveillance. *Center for Democracy & Technology*. Retrieved from: https://stanford.edu/~jmayer/law696/week8/Going%20Dark%20or%20Golden%20Age.pdf

Taylor, P. (2015, October 5). Edward Snowden: Man at the Eye of a Storm. *BBC News*. http://www.bbc.com/news/world-34443844

Trimm, T. (2013, December 23). If Snowden Returned to US For Trial, All Whistleblower Evidence Would Likely Be Inadmissible. Freedom of the Press Foundation. https://freedom.press/blog/2013/12/if-snowden-returned-us-trial-all-whistleblower-evidence-would-likely-be-inadmissible

Trottier, D. (2012). *Social Media as Surveillance: Rethinking Visibility in a Converging World.* England. Ashgate Publishing.

*United States v. Snowden* (2013). US vs. Edward J. Snowden criminal complaint. *Washington Post*. Retrieved from: http://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496/

Wasserman, E. (2015)" Protecting News in the era of Disruptive Sources" in Goldfarb, R. (2015) *After Snowden : privacy, secrecy, and security in the information age*. New York, Thomas Dunne Books.

Wetson, G., Greenwald, G, Gallagher, R. (2014, January 30) CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents. *CBC News*. Retrieved from: http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

Whitaker, R. (2015). The Failure of Official Accountability and the Rise of Guerilla Accountability. Law, *Privacy and Surveillance in Canada in the Post-Snowden Era*. University of Ottawa Press. Canada.

Williams, R. (2005). "Politics and Self in the age of Digital (Re)producibility". Fast Capitalism 1.1. Retrieved from: http://www.uta.edu/huma/agger/fastcapitalism/1_1/index.html

Wyden, R. [Ron Wyden] (2013, March 12). *DNI Clapper Tells Wyden the NSA does not collect data on millions of Americans.* [Video File]. Retrieved from https://www.youtube.com/watch?v=QwiUVUJmGjs

Zuboff, S. (1988). *In the Age of the Smart Machine: The future of work and power*. New York, NY: Basic Books.

Zuboff, S (2013). The Surveillance Paradigm: Be the friction - Our Response to the New Lords of the Ring. *Feuilleton*. Retrieved from http://www.faz.net/aktuell/feuilleton/the-surveillance-paradigm-be-the-friction-our-response-to-the-new-lords-of-the-ring-12241996.html

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology. 75-89.

Zuboff, S. (2016, March 5). Google as Fortune Teller: The Secrets of Surveillance Capitalism. *Feuilleton*. Retrieved from: http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html>

Zygmunt, B., Bigo, D., Esteves, P., Guild E., Jabri V., Lyon, D., and Walker, R., B., J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology* 8 (2): 121-144.

## Works Consulted

Coleman, G. (2011). Hacker Politics and Publics. Public Culture. Vol 23, No. 3, 511-516

Currier, C. (2016, October 21). The U.S. Government Wants to Read Travellers' Tweets Before Letting Them In. *The Intercept.* https://theintercept.com/2016/10/21/the-u-s-government-wants-to-read-travelers-tweets-before-letting-them-in/

Zetter, K. (2013, July 16) Snowden's Contingency: 'Dead Man's Switch' Borrows From Cold War, WikiLeaks. *Wired*. Retrieved from http://www.wired.com/2013/07/snowden-dead-mans-switch/