The Rehearsal and Performance of Lawful Access

by

Jordon Tomblin

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Master of Arts

in

Sociology: Specialization in Digital Humanities

Carleton University
Ottawa, Ontario

Abstract

Lawful access is a carefully calculated legislation to validate existing state surveillance. Drawing on internal government records obtained using Canada's federal *Access to Information Act*, this thesis examines the rise of proactive, intelligence-led policing practices and explores the discursive enactments that reified lawful access (Bill C-13). Based on an investigation of documentary data between 2008 and 2014, I argue lawful access came into force to retroactively legitimize policing aspects of surveillance, which previously contravened Canadian law. Analysis of official (front stage) and unofficial (backstage) data is juxtaposed to explicate rehearsals and performances that constituted the positions of proponents and opponents to lawful access. Unexpected findings of this study include the scope of electronic surveillance that has taken place against Canadian citizens for non-criminal purposes and the common purchasing of user metadata held in telecommunication carrier servers by law enforcement and intelligence communities.

Keywords: Lawful Access, Intelligence-Led Policing, Surveillance

Table of Contents

Abstract ..... **i**

Acknowledgements ..... **ii**

Table of Contents ..... **ii**

1 Introduction **1**
1.1 Research Aims and Research Question 3
1.2 Previous Research on Lawful Access 3
1.3 Thesis Outline 7
1.4 Theoretical Framework 8

2 Exploring Cyber Risk **12**
2.1 Threat Assessment 14
2.1.1 Cybercrime 15
2.1.2 Cyber-terrorism 18
2.1.3 Cyber-warfare 20
2.1.4 Hacktivism 23
2.2 Threat Response 24
2.2.1 Council of Europe's Convention on Cybercrime 25
2.2.2 History of Lawful Access Legislation in Canada 30

3 Theoretical Framework **37**
3.1 Intelligence-Led Policing: From Reactive to Proactive 37
3.2 Policing Developments in the 21st Century 44
3.3 Revisiting Surveillance: 'Welcoming' Big Data 49
3.3.1 The Role of Metadata 52
3.3.2 Proactive Strategies, Retroactive Purposes 56

4 Methodology **61**
4.1 Case Study Approach to Canada's Lawful Access Legislation 61
4.2 Selection of Sources and Data Collection 62
4.2.1 Publicly Available Information 64
4.2.2 Internal Government Records 66
4.3 Data Organization and Presentation 70
4.4 Research Process and Data Analysis Strategy 71

5 Re://Presenting Lawful Access **76**
5.1 Manufacturing Support 77
5.2 Framing Lawful Access as a 'Cyberbullying Bill' 79
5.3 Absence of Investigative Powers? 90
5.3.1 The Scope of Electronic 'Non-Surveillance' in Canada 100
5.4 *R. v. Spencer 2014*, unanimous decision but uncertain effect 112
5.5 A New Way Ahead 117
5.5.1 Fishing Expedition? 121
5.5.2 Minority Report Creep? 124

6 Conclusion **127**
6.1 Recommendations 131

Bibliography **134**

The Internet has developed under a private-sector-led model and has produced extraordinary economic, social and cultural benefits. The governance model has reflected the worldview of western democracies who until recently were responsible for not just developing Internet technology, but also for the majority of Internet content and audience. As more of the world moves online, the number of diversity of Internet stakeholders increases and re-examination of the model is required.

- Department of Industry, 2013 (request #A-2013-00415:1)

1 Introduction

This research project highlights certain potentialities and reverberating effects of a novel surveillance and policing policy in Canada: an examination of lawful access law. It is about the problematizations of aspects of the Web, about those who utilize discourse of crisis to enact new powers into law. It is a project that highlights the resistance between old power ("the physical state") and new (digital) power ("the cyber state"). In particular, it explores the rise of proactive, intelligence-led policing practices in Canada and argues that the Government's recent lawful access legislation's royal assent into law legitimizes (i.e. it is a form of retroactive legalization) of many policing aspects of surveillance, in relation to unlawful third-party user metadata disclosures and the investigation of citizens for non-criminal purposes. I argue Canada's lawful access legislation embodies a number of tenets that negatively impact notions of personal privacy and in many ways, doing so in manners that previously contravened the law. Drawing on evidence obtained utilizing Canada's federal *Access to Information Act,* I aim to move beyond politics-as-usual from left and right state representatives 'informing' publics about what lawful access seeks to do and why the law ought to exist by presenting two complementary, intersecting vantage points: 'front stage' and 'backstage' discourse (Goffman 1959; Walby and Larsen 2012). To this extent, I explore (1) some of the personal consequences of existing within a more technology-mediated society, (2) how law enforcement agencies keep watch on activities

of everyday life and (3) how recent a shift in policing policies have been legitimized via official (front stage) and unofficial (backstage) state discourse.

Erving Goffman's (1959) powerful dramaturgical metaphor for social interaction around the *front stage* and *backstage* as a concept to explicate the roles that individuals or groups perform toward various audiences is one that runs throughout this thesis project. The 'front stage' of government is directed to public audiences through multiple vantage points: legislative and senate debates, media, campaigns, etc. The 'backstage' is where government performance is carefully produced and rehearsed; it is obscured from public view, as public access is often denied, but it can studied by looking at specific *objects* of texts generated in day-to-day government functions: emails, BlackBerry Messenger Pins, internal reports, commentary, etc. This thesis provides 'partial entrance' (see Walby and Larsen 2012) into the backstage of certain Government of Canada (GoC) departments by analyzing and representing some of the activities behind the wide veil of state actions by using access to information requests, which can provide internal state records that were not previously available for the public's consumption, as they were not voluntarily given. These records were requested, paid for, and ultimately negotiated for their release. With this data, I analyze 'front stage' discourse against 'backstage' texts surrounding Canada's lawful access legislation, Bill C-13, or the *Protecting Canadians from Online Crime Act*.

Surveillance and power is often said to be an invisible asset and artifact that exists within and beyond individual consciousness while being omnipresent but yet still open to change; power is flexible and rigid (Foucault 1991). This thesis explores the increase of electronic surveillance and Internet policing practices, of which take place outside of our awareness, as many of these activities are governed *through* technology and other private

intermediaries such as Canadian Internet service providers (ISPs). The front stage of our online activities comprises of performances we generate and display to many audiences: be it forum postings on a website or a tweet for the entire world to witness. Behind digital activities is an electronic trail revealing *where* we travel to on the Web, *whom* we interact with, *when* we connect, and in very specific ways, the reason *why* we engage in particular performances; that is, users inadvertently leave traces when using technology that is most often referred to as *metadata*. Recently, governments and law enforcement agencies have sought access to 'backstage' metadata for numerous policing and security purposes. This thesis explores the issues associated with such trends, as the advent of lawful access has raised a number of fundamental questions around the future state of Canadian privacy.

1.1 Research Aims and Research Question

The purpose of this research was to:

> 1. Consider broader questions of how and why lawful access emerged through an evaluation of the ways in which the Government of Canada has 'problematized' policing security shifts via official (public) and unofficial (backstage) discourse,
>
> 2. Interrogate the validity of how a perceived lack of proper investigative tools for Canadian law enforcement contributed to the introduction of lawful access, and
>
> 3. Evaluate the legal, social and ethical implications of lawful access in regards to the privacy of Canadians and other endowed fundamental human rights.

This thesis draws on existing scholarly work in the multidisciplinary subfield of Internet surveillance studies and asks: *why, how and with what effect are intelligence-led policing models being adopted to secure the cyber environment?*

1.2 Previous Research on Lawful Access

This examination has undoubtedly intersected with other social scientific inquiry. In a Canadian context, twelve other scholars from among the social sciences, humanities

and computer sciences have investigated questions around lawful access individually and collaboratively using different vignettes. Escudero-Pascual and Hosein (2002) have both highlighted how discourses surrounding lawful access law are primarily enveloped using technology-neutral language among Western governments. That is, domestic nation state security policies are often framed by broader international conventions, which frequently downplay the highly sensitive nature of metadata telephony information. Consequently, most Western states have attempted to introduce new legal frameworks and investigative powers to security intelligence as well as policing agencies by using ambiguous language and rhetorical techniques, of which inaccurately treat user metadata as being analogous to older telephone system records. This is to say that proponents of lawful access law often digress that the elements of communications protocols of rotary dial aged telephones are no different than the sophisticated modern Internet connections that transmit information.

Huey and Rosenberg (2004) have noted that international cyber-crime prevention frameworks promote the policing of the Internet as a multilateral enterprise requiring the private sector and the public sector to work together. 'Securing' cyberspace consequently necessitates the private sectors to play a role in the *activity* of policing, as ISPs facilitate Internet access and can therefore offer police the necessary user data to govern the Web. Their work has largely underscored the fact that the Council of Europe's *Convention on Cybercrime*—which Canada is signatory to—has given fodder to ignite state surveillance systems beyond our contemporary constraints. This is to say that the Internet provides an arena for facilitating multiple activities of everyday life and to therefore give the police greater access to this data absent of any oversight would provide a means for policing and surveillance to subsist in a way where there is no functional equivalent offline.

Young (2004) argues that government discourse surrounding lawful access law in Canada and abroad has been largely anecdotal: it is predicated on providing a 'necessary' framework for police to address technology-mediated crime. Still, his work notes that the Canadian federal government's arguments regarding the rationale for such introductions depart markedly from any empirical evidence that would highlight its genuine necessity. His research emphasizes the fact that lawful access' legal force and effect may in fact *be* a panacea for proactive crime prevention, but in doing so it would annihilate any present understandings of personal privacy and would create panoptic surveillance infrastructures delivered by private sectors (e.g. ISPs) for various government agencies in consequence.

Other researchers have also tangentially engaged in debates around lawful access. Beardwood (2003) has provided analysis of the three controversial tenets, as articulated in the GoC's consultation document when lawful access initiatives were first forwarded. Shade (2008) offers a comprehensive overview of increasingly invasive trends that have undermined Canadian privacy since 9/11 from the heightened concerns around terrorism heading a call for anti-terror legislation to the general insecurities around information and communication technologies (ICTs)[1]. Mann (2009) highlights the legal and technological implications of covert and remote intelligence collection by police for potential suspects through the use of Trojan horses and other such malicious software by representing some unintended effects of said policing tools. Roe and Bail (2012) underscore the importance

[1] Evidence and recent activities (e.g. *the Islamic State of Iraq and Syria* or *Boko Haram*) highlight the realities and devastating effects of terrorist actions. In response to these foreign activities, Canadian citizens have witnessed Governmental responses that denote anti-privacy measures, which may be an unduly and unfair reaction to the circumstances overseas or to domestic events, which are no different than inter or intra gang violence. I do not however downplay the real threat and effect terrorism can have on a country.

of being able to freely disseminate information and argues that an onus rests on librarians to teach the public about varying privacy issues and implications of invasive, impending policy proposals. Swire (2012) presents optimistic and partly effective means to disrupt the efficacy of lawful access: implement strong end-to-end encryption. He anticipates that given the creativity of software developers and computer programmers globally, product innovation in every day technologies can be purposely designed to evade state as well as corporate surveillance thereby making lawful access legislation moot[2].

Trottier (2012) examines the previous iterations of lawful access proposals, which like in its present form, grant law enforcement greater access to metadata that can be used alongside open-source intelligence (OSINT) collection of voluntarily generated, publicly available communications content on social media website(s)[3]. In other words, the police can frame a particular picture of a potential suspect by combining publicly available data against backstage, involuntarily generated user metadata. To this end, enhanced visibility of one's social life may contribute to profiling or predictive policing. Witaker (2012) has highlighted the fact that since the tragic events of 9/11 there have been resounding calls by Western governments to reign in lawful access laws and to expand policing powers to the Web. Yet despite the efforts by both Liberal and Conservative governments, frequent party turnover has hitherto hindered Parliament from establishing its tenets into Canadian

---

[2] Despite the optimism of Swire, recent leaders of 'liberal' secular democracies, such as Prime Minister David Cameron of the United Kingdom, have proposed to ban encryption altogether in order to deny criminals or terrorists "safe spaces" for communication on the Internet (Watt and Wintour 2015). Such a move would of course equally deny any citizen from communicating securely and privately online whereas surveillance would become more ubiquitous and their citizens would more easily be subject to other surveyors.

[3] As Stephen Mercado (2009) and Wesley Wark (2013) have documented, open-source intelligence (OSINT) constitutes the majority of "intelligence" (i.e. information utilized for a particular purpose) for security intelligence and law enforcement communities.

Law. Finally, Christopher Parsons (2015) has examined the lack of transparency among Canadian ISPs for communicating to their subscribers how many metadata requests they receive annually and the level of compliance in their disclosures. He argues, "At the end of 2014, we have more pieces to the domestic surveillance jigsaw than ever-before. But to complete it more context about the dimensions of the puzzle itself is required" (16).

This thesis provides additional pieces to the contemporary issues of lawful access, Internet surveillance and policing done digitally. I offer a distinctive theoretical lens and application to describe the trend toward proactive policing models in Canada and argue that what we are witnessing is a form of broad, Big Data surveillance being facilitated by intelligence-led paradigms. Employing a seldom-used methodological tool in the social sciences, I utilize access to information (ATI) requests to explicate the salient differences around the 'official', front stage discourses of the state against the 'unofficial', backstage texts as artifacts of study. Moreover, I analyze variegated discourses of parliamentarians and interveners at legislative stages that constituted Canada's lawful access legislation.

1.3 Thesis Outline

In chapter two, I present the groundwork around the policing of the Internet. This chapter outlines major threats and issues associated with activities that take place online and predominant, tentative responses by the state. It highlights the transnational Council of Europe's *Convention on Cybercrime*, but focuses on providing a historical overview of lawful access in Canada. Chapter three offers a theoretical discussion around intelligence-led policing. I present this framework to explicate how these security policy shifts toward lawful access reflects broader moves from more *reactive* policing paradigms toward more *proactive* data-driven efforts in the context of an information society. I situate discussions

in policing and surveillance studies literature to explore potentialities of intelligence-led policing, as agencies shift from offline, people-focused and targeted forms of surveillance toward online, metadata-focused and dragnet bulk data collection to maintain social order and to keep watch. That is, social problems are increasingly viewed security problems.

Chapter four outlines the methodology. In particular, I introduce one case study to explore this emerging phenomenon and discuss the critical significance of using *Access to Information* requests to examine 'official' and 'unofficial' discourse. In chapter five, I present three of the major themes that arose from the analysis. Chapter six then concludes this thesis by rearticulating the central arguments and exploring some of the more broader sociological implications of contemporary policing and surveillance trends around lawful access' real and hypothesized effects on Canadian privacy while proposing several ways to hack these shifts. I argue that while Internet surveillance is increasingly omniscient and omnipresent, the government and its mosaic of law enforcement agencies will continue to discriminately target certain individuals and seek out electronic pattern of behavior based on social constructions of threat, which might have more to do with (biased) policing-led intelligence rather than intelligence-led policing.

1.4 Theoretical Framework

This thesis is associated towards an analysis of surveillance and policing around lawful access legislation rooted in a focus on the *texts*, the *work*, and *networks* of various GoC agencies involved in the production of order maintenance (Walby and Larsen 2012; Haggerty and Ericson 2000). Specifically, it chronicles the social construction of lawful access as a necessary and proportional framework to help 'secure' the cyber environment. The analysis juxtaposes 'official' discourse against the production of the 'unofficial' texts

manifested within the day-to-day processes while exposing backstage federal activities to help understand how meaning, discourse, phenomena, language and symbols are socially constructed in each of these dialectical positions (Gergen 1999).

Social constructionist perspectives are most often concerned with explorations of how people comprehend and order their world by (in)actively operationalizing it in social and culturally bound contexts (Charmaz 2006). The conceptual underpinnings denote that multiple constructions of the world are inevitable and that there are no Truths – "truth claims" derived from data analysis is an edifice of the individual researcher's positioned perspectives (see Gergen 1999:63). Specifically, I utilize a constructivist grounded theory approach, influenced by frameworks articulated by Charmaz (2006) to rigorously analyze the case study from 'front stage' and 'backstage' vantage points[4].

Understanding the presupposition that the law, like any social artifact, is a social construction embedded within cultural traditions, this thesis concerns itself with an actor-oriented approach to engage in the broader discussions around lawful access on Canadian personal autonomy. I explore the discourses of actors—Members of Parliament, experts, senators, judges, professors, etc.—made in legislative processes around the advent of Bill C-13 against certain *texts*—PowerPoints, emails, internal memos, etc—obtained through Canada's federal *Access to Information Act*. In doing so, it draws upon the dramaturgical work of Erving Goffman (1959), as open-government activists and access to information scholars have presented it as a useful way to "study negotiated meanings and moments of impression management" (Walby and Larsen 2012:37) by describing and highlighting the complexities around the emergence of particular phenomenon.

---

[4] This will be covered in detail in Chapter four.

Goffman (1959) presents a sophisticated conceptual framework to (re)present the extent to which individual actors *appear* before others through expressions of language, symbolism, behavior, verbally and non-verbally albeit in overt, covert and/or aggressive or passive-aggressive forms. Influenced by William Shakespeare's famous epic that "all the world's a stage", Goffman explores some of the hidden meaning of human action and communications (by expressions *given* and expressions *given off*) through the 'products' one offers to a public audience (136). Goffman's model presents distinct opportunities to study formations of official GoC discourse against unofficial communiqués or products.

Writing from the position that all individuals are merely actors or 'players' on the world's stage, 'official' discourse allows us to study the 'front stage' of government: the place(s) where performances are given under specific circumstances (13). Meanwhile, the 'unofficial' backstage activities: the place(s) where "impressions are openly constructed" (69) and where "performers behave out of character" (70) become observable through the documentary data generated from using Canada's *Access to Information Act*.

It is here, the backstage, which presents opportunities to study the 'products' of a "presumably unintentional kind" (138); that is, the "official texts that are never intended for public circulation" (Walby and Larsen 2012:33). To this extent, the study of some of these socially constructed texts can allow us to explicate how the government informs the general public "as to what [something] is" (such as lawful access) and "as to what [we the public] *ought* to see as the 'is'" (Goffman 1959:144).

Inspired by theoretical additions to this perspective by Jeffrey Alexander (2004), I draw from his cultural pragmatics model to study government performances to the extent of "why" and "how" they ascribe meaning to the social situations of lawful access in their

public displays. Moving past performative gestures channeled vis-à-vis official networks background representations and scripts of these carefully manufactured communiqués are imperative objects of study to explore relationships of apparent clamor and truth claims.

Alexander's theoretical model highlights the fact that in the contemporary society, state performances are often subject to questioning in proportion to their authenticity like never before. This is due part to the level of global and local access to information today (e.g. with the advent of the Internet) and multitude of channels that facilitate information dissemination and permit knowledge acquisition. For performances to be accepted as an authentic exposé, the social and cultural elements require synchronicity and order; that is, "the elements of social performance" must be *fused* together (32). The performance must be remarkable and convincing. The more disparate and divergent a social performance is, the "elements of performance" come to be regarded as *de-fused* and so "becomes subject to institutions of independent criticism" or peripheral de-legitimization (69). Combination therefore of A) public discourse and B) access to information records allows us to study the validity and legitimacy of prevailing state assumptions around lawful access, which presupposed that the Internet is a dangerous place that cannot be managed except through additional legal frameworks for state and non-state actors.

This study advances by interrogating the *rehearsal* of lawful access legislation via 'backstage', unofficial textual artifacts (i.e. access to information requests) and the state's *performances* on the front stage; that is, carefully crafted 'official' discursive enactments, which sought to legitimize and reign in 'new' policing aspects of surveillance in Canada. But before those discussions take place, the next chapter situates lawful access among the multiple constituents and events that constituted its emergence and fueled its prominence.

2 Exploring Cyber Risk

Risk is an omnipresent actor in society. It is transformational and performative: it can be representative and ascribed to any person, thing, institution or philosophy along a continuum of being regarded as either "more or less risky" (Beck 2009:3). It is malleable and prescriptive, and it often requires stakeholders of risk management or risk aversion to respond to 'it'. Risk can be negative in so far as it can generate fear(s)—imagined or real harm—but yet also presents positive effects and potentialities. As Ericson and Haggerty (1997) argue, risk "provides [the] bare-minimum truths that reality is certain", but yet our 'knowledge' of it can produce new risks, which can be measured or constructed through "scientific knowledge and technologies" as *sources* of risks and yet also be "the primary basis of security efforts aimed at controlling such risks" (89).

The Internet and related tangential information and communication technologies (ICTs) have equally become omnicompetent actor in most societies. As Ralf Bendrath (2001) argued over a decade ago, the "information society" is "showing significant signs of being a 'risk society'" (81). According to Ulrich Beck (2002), the idea or perhaps even the epitome of the 'risk society' is that, "The speeding up of modernization has produced a gulf between the world of quantifiable risk in which we think and act, and the world of non-quantifiable insecurities that we are creating" (40). Contemporary questions around cybercrime, cyber-terrorism, cyber-war, and hacktivism have come to dominate everyday discourses around public order and crime prevention. Despite the rise and significance of these emerging discourses, which can be observed in both official government reports to popular media exposés, 'cyber issues' generally remain poorly understood theoretically

and empirically. Still, varying social justice[5] implications of these activities are becoming increasingly profound in terms of how governments respond to these 'risks', as particular state responses have made the lives of citizens on the Internet more transparent to actors of policing and security order maintenance.

As Ericson and Haggerty (1997) both argue, "privacy, trust, surveillance, and risk management go hand in hand in policing the probabilities and possibilities of action" (6). This thesis is concerned with the discussions around these intersections in regards to how lawful access in Canada was socially constructed as both a 'necessary and proportional' framework to mitigate cyber risks by providing law enforcement and security intelligence agencies with the proper tools to 'secure' the cyber environment. Specifically, it looks at the rise of Big Data policing practices in Canada and how user metadata has become an invaluable currency for proactive policing purposes.

Before these discussions take place, this chapter firstly presents four predominant 'cyber' risks, which have (re)emerged in the context of the Internet and as edifices, which have framed Government of Canada (GoC) debates around the need for lawful access. Secondly, it situates Canadian circumstances in a broader international context, as lawful access legislation descended from larger legal conventions and historical alliances, which promote domestic framework implementations among allies. This proposal materialized out of an understanding that the Internet has developed into a boundless 'Third space' (Wall and Williams 2007) beyond public and private life *offline*. This has prompted many Western states to adhere to the international tenets forwarded by the Council of Europe's

---

[5] Referring to social justice as it relates to quenching individual freedoms and personal privacy through invasive (cyber) security policing apparatuses.

Convention on Cybercrime, which establishes that due to the jurisdictional limits that can impede the police and national security forces from governing in foreign states, countries should develop frameworks that reflect international guidelines to enhance cybersecurity. In other words, given that cyber actions are peripatetic in nature and the Internet allows us to connect to different 'spaces', which may then 'exist' in a different country, nations require ways to prosecute and detect activities that emanate outside of their jurisdictional authority. The final section highlights lawful access developments in Canada. It maps out chronological progressions and failed attempts that have culminated for over a decade. It covers the most pertinent sections regarding later discussion on privacy, surveillance and policing of the Internet.

2.1 Threat Assessment

For decades, Canadian media has frequently informed the public that cyber issues are escalating and that the Government may not be prepared for a wide scale cyber event. The following illustration of select news media headlines represents an ever-worsening picture: "Blame Canada for 80% of cyber-attacks: Country a 'zone of vulnerability,' U.S. Military Report Warns" (Pugliese 2000), "Canada losing the battle on cyber crime, experts say" (Regan 2006), "Canada unprepared for massive cyber attack: expert" (Pilieci 2010), and "'Cyber version of Pearl Harbor' looms over energy industry; security expert warns Canada at risk" (Gignac 2013). While these sensational narratives remind us that news media exists on one hand to generate profit and do not necessarily carry an onus to present the public with facts, it is important to explore such topics as citizens principally form their opinions from news media depictions (see Greenberg 2000) and nation states

often respond to citizen's fears in order to maintain the status quo and to demonstrate that action is being taken in response to social, political or economic risk whether real or not.

As Haggerty and Ericson (1997) argue, "Problem-solving policing is the basis for constituting the police as knowledge brokers that are more directly responsible for governance" (190). As Jean-Paul Brodeur (2007) has contended, the terms "policing" and "governing" were originally synonymous but yet are too often associated as being distinct (26). This section presents a threat assessment of various neologisms, which have come to dominate discourses around the motif behind the reigning in of lawful access law. It is principally framed through Brodeur's distinction between *high policing* structures, which regards agents of the state protecting the "political order" of things versus *low policing structures*, of which regards governing the deviant activity that is not of a kind that would undermine macro social structures (i.e. the majority of street crime).

2.1.1 Cybercrime

Cybercrime is a concern, which regularly captures the interests of news media, the public and the government. In Canada, the most widely used definition of cybercrime is forwarded by Statistics Canada[6] (2002), who uses the Canadian Police College definition**:** cybercrime is "a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence" (6). Statistics Canada's description is also consistent with the two-cybercrime categories forwarded by Canada's

[6] Statistics Canada is one of twelve federal departments constituted by Industry Canada. The agency is authorized and "required to collect, compile, analyse, abstract and publish statistical information relating to the commercial, industrial, financial, social, economic and general activities and conditions of the people of Canada" (2015:N.P.).

highest federal and national police force, the Royal Canadian Mounted Police (RCMP): technology-as-target and technology-as-instrument[7] (2014:3).

Alana Maurushat (2013) argues cybercrime is a term to define traditional criminal code offences that could be "committed or enhanced by technology such as the Internet" (120). Meanwhile, a commissioned Parliamentary paper on the topic of cybercrime notes, "Although much is being said about cybercrime, there is not unanimous agreement on a single definition of the concept" (Valiquet 2011:1). As with many concepts, 'cybercrime' lacks definitional clarity. Still, Maurushat (2013:120-121) offers us a coherent description that is adopted herein for the purpose of this thesis,

> Cybercrime covers four general areas protected under the international *Convention on Cybercrime* and by most domestic law frameworks in the Asia-Pacific region…1) fraud and forgery 2) child sexual abuse materials (child pornography) 3) copyright infringement (intellectual property) and 4) computer offences (involves a form of hacking) / unauthorized access and use of data, data systems and computers.

In 2004, the internationally used Uniformed Crime Report (UCR)[8] classification schema was amended to include computer offences as *distinct* criminal infractions and created the means to count traditional common-law offences facilitated by the Internet and computers (Statistics Canada 2014a). Criminal threat assessments are only as accurate as the systems devised and able to count them (see Skogan 1977). Criminologists have long understood

---

[7] The RCMP (2014) state, technology-as-target concerns "criminal offences targeting computers and other information technologies" whereas technology-as-instrument refers to "criminal offences where the Internet and information technologies are instrumental in the commission of a crime, such as those involving fraud, identify theft, intellectual property infringements… [etc]" (3).

[8] In Canada, the Uniformed Crime Report is used to measure incident-based, police-reported crime statistics such as the criminal code infraction(s), the characteristics of an offence(s), the victims (if any) and the person(s) accused (Statistics Canada 2015). The collection of UCR data is used for crime analysis and informs police resource allocation.

this argument and this specific line of reasoning may not necessarily differ in the context of the Internet and technology-mediated offending. In 2012, reported cybercrime incidents accounted for a rate of 33 incidents per 100,000 individuals (Statistics Canada 2014b). In comparison to *offline* crime, there was a reported 5,588 incidents per 100,000 individuals during the timeframe (Statistics Canada 2013). Despite this, the Government has proposed multiple legislative frameworks and legal tools to keep the 'issue' of cybercrime at bay[9]. Stohl (2007) has argued that this trend is expected, "Governments engage in the creation of systematic studies and blue ribbon panels, none of which are likely to report that they can guarantee that no threat exists and that it won't grow larger in the future for fear of looking weak or contributing to a state of unpreparedness" (225-6). While we can infer therefore that the Government has been proactive in their response to cybercrimes, the outstanding question is whether the Government has been heavy-handed. In Canada, for instance, the birth cohort studies (Tremblay et al. 2003; Carrington et al., 2005; Matarazzo 2010) and established age-crime curve (Brodie 2008) have consistently shown that even in the absence of intervention, the majority of offenders desist in offending as they age. It also remains to be seen whether such responses warrant surveillance legislation and other similar Acts, which provide greater powers to law enforcement and security intelligence agencies while the lives of Canadians become more transparent (see Bennett et al. 2014) In addition to cybercrime, questions of *cyber*-terrorism have equally garnered notoriety.

[9] To this degree, the Government has been proactive in their approach where no doubt the public often complains of the sluggish pace of proposal enactments, which are largely done retroactively following some event or crisis. The issue here nonetheless is that the reactions toward cyber issues, which statistically are few, may indeed be an overreaction.

2.1.2 Cyber-terrorism

Whereas Stohl (2007) argues, "consensus among security experts is that there has never been a recorded act of cyber-terrorism pre- or post-9/11" (224), cyber-terrorism has still been represented in news media and GoC reports. Dorothy Denning explains (2000),

> Cyber terrorism is the convergence of terrorism and cyberspace... Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures *could* be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not (emphasis added, 1).

Said differently, cyber-terrorism can be understood as the purposeful use of violence to achieve "political objects" or to generate fear through technology (e.g. the Internet) while "meet[ing] certain psychological needs of those who are attracted to terrorism" (Lewis 2003:36). As Weimann (2004) notes, cyber-terrorism discourses erupted in the wake of 9/11 in security and policing studies and among Governments. The advent of the New Millennium (or Y2K)—which was predicated on an idea that old, outdated technology, which had not been properly programmed to account for a date-time change from 1999 to 2000 would deliver us chaos—further exacerbated fears around the unknowns or black boxes of technology (Stohl 2007:224). Still, these debates frequently depart from "what a computer attack *could do*", but yet seem to be all "too often associated with what *will* happen" (225). Richard Lazarus proposes this is due to the fact that the *terms* 'cyber' and 'terrorism' individually have come to be two of the modern fears that have now defined aspects of contemporary society (as cited in Stohl 2007:225). The amalgamation of these two neologisms therefore erupts a positive amount of uncertainty and discontent.

Cyberterrorism is also frequently associated with notions of an 'electronic Pearl Habor'. As Stohl (2007) notes, technology novelist, Winn Shwartau, first pioneered that

term, with his book *Terminal Compromise: Computer Terrorism in a Networked Society* in attempt to increases his sales. Meanwhile, the actual term cyber-terrorism is credited to Barry Collin who, in 1982, hypothesized that critical infrastructure such as transportation vehicles (e.g. airplanes and cars) could be disabled *through* technologies (Denning 2010). It is perhaps no surprise then that the once-popular Hollywood film *WarGames* in 1983—which depicted a young skillful hacker who inadvertently accessed an American military supercomputer, nearly causing a nuclear attack—is immortalized into popular culture.

Weimann (2004) has argued, "An entire industry has emerged to grapple with the threat of cyberterrorism" from think tanks to formal presentations delivered before the highest structures of the Government (3). Despite this, Lewis (2003) remarks that while cyber-terrorism has garnered much notoriety, it has "meant little more than propaganda, intelligence collection, or the digital equivalent of graffiti, with groups defacing each other's website" (37). Conway (2014) notes that the social construction of this 'threat' is predominantly associated with hypotheses around the potentialities of technology rather than any sound empirical evidence. Others have also looked at the economic impacts of cyber-terrorism, of which often conclude that greater security investments in information systems technology will help to curtail the costs and impacts of a catastrophic event (Hua and Bapna 2012). Nonetheless, much of this literature is dominated by the 'what ifs' of occurrences. Although Denning (2011) and Weimann (2004, 2008) equally acknowledge that cyber-terrorism is a real threat; calculation of any such risk along a continuum will only be more accurate *if* we begin to witness such activities emerge in the years ahead.

As Peter Singer (2014) has reminded us however, "Squirrels have taken down the power grid more times than the zero times that hackers have" (N.P.). This warrants him

to ask if governments are failing to create effective responses and whether this is causing an "imbalance in how we structurally respond to [cyber] threat[s]" today (ibid). In the comparing of the Internet as a practical agent to deliver terrorism, Stohl (2007) notes that this medium must also therefore "produce similar or greater results for less effort than a conventional one" (233). In other words, given the high sophistication necessary for one to have in terms of computer virtuosity needed to carry out such an event that may indeed "undermine confidence in the political structure and create difficulty within the body politic" (237), its unlikely that such an attack would emanate from terrorist groups today; explosives require less effort, training and skill than a cyber attack. Moreover, both state and corporate surveillance of online activities are arguably better equipped to detect such acts of cyber disobedience than the surveillance of non-cyber activities. Still, it is evident that the Internet can and *is* used as a recruiting tool for terrorism groups (e.g. seen in the recent activities of the *Islamic State of Iraq and Syria* or ISIS). However, such use of the Internet is of course no different than non-criminal or non-malicious usage as a means for recruiting, fundraising or developing operational plans (Gendron 2013). Still, the fear of cyber-terrorism is not lost and is often accompanied by discussions of cyber-warfare.

2.1.3 Cyber-warfare

War and technology are two defining characteristics that transcend the history of humanity. Clarke and Kanake (2010) have argued that cyber-warfare involves "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (6). This understanding is congruent to Alana Maurushat's (2013) work, arguing cyber-warfare consists of the "actions taken to affect an adversary's

information and information systems while defending one's own", of which is most often "initiated through government infrastructure or state-sponsored" attacks (121).

In one PowerPoint presentation made available through Canada's federal *Access to Information Act*, an internal Public Safety Canada (request #A-2011-00143) document dated to 2011 states that indeed, there is "No normative code regarding whether the use of a multitude of (malicious) network activities represents a Use of Force, equivalent to an Armed Attack" offline (7). Further, "There is no clear/common understanding of the military role in the cyber environment across the spectrum of traditional military" (ibid).

While the meaning of what is meant by the "spectrum of traditional military" is an known unknown (see Rumsfeld 2002), leaks made available by American whistleblower Edward Snowden, *do* provide evidence that the Canadian military's "normative code" on their role on the Internet has changed since 2011. Indeed, as Gallagher (2015) highlights, evidence has now emerged that the Communications Security Establishment Canada (or CSEC) has engaged in what could well be understood as cyber-warfare, with their attacks against the information systems of Mexico and Northern African governments. Today, it is unclear whether academics can continue to argue that there are no empirical records of cyber-terrorism acts, which could also equally be framed as acts of cyber-warfare in light of these disclosures. This case raises questions around CSEC's mandate, as they took up an active military and an offensive role in cyberspace whereas CSEC is *theoretically* only responsible for collecting, analyzing and disseminating "intelligence" on threats related to national security for law enforcement partners according to their current mandate[10].

---

[10] CSEC (known also as the CSE) once had "no governing statute setting out its mandate, powers and control/accountability mechanisms" but has always been primarily concerned

It appears that while there is legitimate concern around perpetration of cyber-war or cyber-terrorism, evidence shows that governments have been behind any empirically observable actions to date. *Stuxnet,* for instance, is considered to be one of the first cyber weapons with capability to damage tangible critical infrastructure systems while also not requiring any Internet connectivity in order to function (Gendron and Rudner 2012:40). Yet, it is alleged that Stuxnet was developed by the American and Israeli government to attack the Iranian nuclear program and nuclear centrifuges in order to disrupt "illegally obtained" devices and "illicit research" perceived to be present (see Singer and Friedman 2014:120). Maurushat (2013) highlights that the Russian government has also used the quite easily executable distributed denial-of-service (DDoS[11]) attacks against the states of Estonia and Georgia in 2007 and 2008, respectively. Within Estonia, the cyber attacks "crippled" the online infrastructure and impacted banking systems, causing "enormous impacts on the Estonian economy for years to come" (119). Meanwhile, attacks against

---

with the responsibilities of capturing "Signals Intelligence (SIGINT)", which is offensive in nature, and "Information or Communications Security (INFOSEC or COMSEC)", which is defensive in nature, as the latter involves protecting Canadian information and communications transmissions (Rosen 1993). Today, the mandate of CSEC is set out in section 273.64(1) of Canada's *National Defence Act*. No where however does it mention or include stipulations regarding offensive actions, such as those taken against Mexico or Northern African governments, where CSEC hacked into both government and corporate networks (see Gallagher 2015). Although an official response by CSEC to the Canadian Broadcasting Corporation noted, Snowden's disclosure do "not necessarily reflect current CSE practices or programs" (Hildebrandt, Seglins and Pereira 2015), Rosen stated back in 1993, that the "CSE is one of the most secret and secretive organizations in Canada" and perhaps remains so. It is therefore difficult to ascertain the validity of their 'official' response or any nefarious activities, as CSEC is enshrouded in secrecy and protected by barriers of opacity (e.g. *Access to Information Act, Privacy Act, National Defence Act*).

[11] According to Maurushat's (2012) report prepared for Public Safety (request #A-2012-00113), a DDoS attack is the equivalent of a "sit-in blocking access to a building" or "a protest which prevents people from using a street" (11). A DDoS is when a system or network receives too many requests from external users asking for access to its services.

Georgia were carried out "the night before Russian troops invaded" the 'physical state' therefore preventing media agencies from reporting on events for days thereafter (ibid)[12].

2.1.4 Hacktivism

Considerable debate has also erupted around the idea of hacktivism, which is the combination of computer hacking and digital activism. Over the years, this term has been misunderstood and much maligned. Originally, hacktivism was put forward as an idea to conceptualize the connection of technology and human rights efforts. It was presupposed in the early 90s that if the Internet increased in presence and scope, it would be a viable means to facilitate political participation, protest and expression. Hacktivism as a concept was firstly linked to the United Nations Declaration of Human Rights and International Covenant on Civil and Political Rights, according to the founder of the term, a computer hacker that goes by the screen-name (i.e. moniker) 'Omega' (Oxblood Ruffin 2004:N.P). The idea behind hacktivism was that social and political change did not require people to assemble in the physical streets and to rally around a cause(s) to provoke transformations: social or economic *adjustments* could emanate from just one, skillful hacker. Despite this powerful ideal and insurrectionist tone, original conceptualization accounted for a need to develop clear ethics and rules of engagement for hacktivist activities (see Oxblood Ruffin 2004). A common illustration of hacktivism is seen in the activities of "Anonymous".

Anonymous is a loosely associated hacktivist collective that is "difficult to pin down", according to Gabriella Coleman (2013:3). Technically, Anonymous is more of an *idea* than it is a group. There is no formal membership, no one leader or clear hierarchical

---

[12] These actions would be consistent with original definitions and understanding of "terrorism"; that is, *state*-driven attacks against citizens causing terror (Primoratz 1990).

structure. It is an international, decentralized collective that has gained notoriety in the press and has captured the attention of many governments. It is a collective that operates much like hamadryas baboons; there are splinter cells that make up the larger collective but their activities are most often ascribed to small but intimate clans[13]. What bring users towards the *hive* of Anonymous are collective ideals: participants are united by the notion that information should be accessible and free speech should be unfettered, especially online (see Olson 2013). There are also overarching beliefs that surveillance is expanding and that citizens of the Internet are able to generate social and political transformations with contemporary technologies at their disposal; that is, of course, in addition to more traditional action. Accordingly, governments around the globe—not just within Canada—regard hacktivism to be a serious risk to the cyber-environment. As a secret PowerPoint (request #A-2014-00010:4) presentation by Canada's cryptological agency, CSEC, notes, criminals are regarded as the biggest threat to the cyber environment whereas hacktivists and state-sponsored actors are tied in second place. Meanwhile, terrorists are the slightest concern. There is no doubt however that each of these actors' position shifts overtime.

2.2 Threat Response

As a consequence of these multiple compounding risks that have emerged within the cyber environment, the Government of Canada—and foreign states—has searched for new technologies of power (i.e. policing tools and legal frameworks) to respond to these

---

[13] As Abeglenn's (1984) research notes, the social makeup of the hamadryas consists of smaller, autonomous units when it comes to foraging patterns and socialization processes (197). Meanwhile, their social interactions and clan formations persist through "leader-follower associations" (ibid). An analogy is set here between the hamadryas and Anons (i.e. those associated with Anonymous), as their 'organization' is most often constituted by individual efforts and actions (protest or otherwise), which can affect particular bonds.

circumstances. At present, the most thorough framework forwarded in this regard is the *Convention on Cybercrime* (2001). The next section details this international framework, as it has become perhaps *the* external driver to advance lawful access in Canada.

2.2.1 Council of Europe's Convention on Cybercrime

The Council of Europe's *Convention on Cybercrime* (hereafter the Convention or the CC), proposed in 1997 and put into effect in 2004, was the first international treaty to confront issues around jurisdictional authority for the purpose of mitigating cyber threats (Weber 2003). The basis for this policy proposal stems from intergovernmental debate in the European Union to help establish standardized implementations for lawful access law across distinct governmental structures (see Frost & Sullivan 2011). The CC was created with an intent understanding that economic and social relations are increasingly mediated through electronic means and that certain cyber activities are inevitably straining the legal systems ability to keep pace and respond using conventional procedural mechanisms.

As Weber (2003:426-7) has noted, the CC addresses questions around jurisdiction of policing by indentifying three, intersecting shortfalls: (1) lack of criminal statutes, (2) lack of procedural powers, and (3) lack of clear enforceable mutual assistance provisions among its members[14]. Stated briefly, the Convention was created to harmonize individual state laws, to address certain known legal constraints and to improve existing information sharing practices among partner governments. Frost & Sullivan's (2011) research report articulates that the CC assists in creating international standards-based models to create interoperability between law enforcement agencies and systems networks (i.e. TSP/ISP),

[14] Mutual legal assistance provisions and letters rogatory (i.e. request from a court in one country to another) promote international cooperation for the apprehension of offenders.

of which provide subscribers with Internet access and other services. Their report further argues that, "The trend is unmistakable: service providers will be required to support law enforcement and intelligence gathering with an increasing amount of data across the entire array of service offerings and technologies" (2)[15]. The Convention therefore seeks to provide legal mechanisms to enhance visibility of apparent peripatetic, digital activities among members. It encourages each member to legislate additional investigative policing powers to mitigate cybercriminal or cyber disobedient activity by strengthening collective cyber-security dexterity of members as a whole and independently. In Canada, such goals and articulations are reflected in lawful access legislation proposals. The preamble of the Convention presents a clear cyber criminal profile and also positions itself as a solution to the detrimental effects of potentially nefarious digital activities on social life:

> New technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society (Explanatory Report to the Convention on Cybercrime, 2001, paragraph 6).

---

[15] Frost & Sullivan's (2011) whitepaper on lawful access and interception was made available through an internal leak posted to the whistle-blowing website "WikiLeaks". Their report provides a comprehensive, corporate approach to manage communications interception technology and is a compelling overview of various corporate drivers that market product solutions for state-sponsored spying via corporatized technologies that can be embedded within existing infrastructures (e.g. TSP or ISP networks). This report symbolizes two things: (1) it provides an additional element to study lawful access law through 'backstage' documents not previously available and (2) highlights the fact that through the values of transparency and openness of the 'leakers' that made this document publicly consumable, we can begin to understand issues of surveillance and policing beyond 'front stage' and 'backstage' government and non-governmental discourse by introducing 'backstage' corporate exposés to understand that indeed a clear enterprise exists around lawful access and state-driven, corporate facilitated surveillance.

The description of these new circumstances indicates that contemporary crimes facilitated by technology are unfastening previous constraints of law and society. The CC therefore encourages both a widespread adoption and development of new instruments—legal and technical—to meet some of these challenges at the forefront of European society and the world writ large. It also encourages international unity and stresses the need for increased visibility mechanisms to exist in order to enhance the apprehension of potential suspects and to improve security. As Frost & Sullivan (2011) argue, its about creating "transparent surveillance" in the sense that "the target must not be able to detect that he or she is being monitored" (6) therefore requiring "the majority of the interception obligations" (13) for surveillance, as an 'onus', to be on corporate providers (i.e. ISPs and TSPs). Accordingly, the Convention is an effort to 'responsibilize' (see Garland 2001) corporate actors to play a critical role within the *activity* of 'policing' the Web whilst ensuring and establishing certain legal and regulatory procedures in order to legitimize (i.e. lawfully) intercept and capture electronic communications. Said another way, the CC encourages governments (individually) to reign in the *Convention on Cybercrime's* tenets into law, otherwise law enforcement agencies will be left with perceivably outdated tools and procedural powers to address these known 'risks' at the fora of the Digital Age. Otherwise, governments will be pitted in a legal quagmire if they attempt to create one-way 'transparency' unlawfully.

Borders have never restrained crime. With the advent of digital technologies and ubiquitous presence of computing and the Internet today, governments are well aware of the fact that prior understandings of criminal jurisdiction, for instance, necessitate new conceptualizations as digital applications continue to unfetter citizens from the domiciles

of every day life. Within the Canadian context, the *Convention's* goals are consistent with official declarations made by the RCMP (2014:14) regarding their address to cyber risks,

> Criminal activities in cyberspace are complex and often transnational in character, where potential evidence is transient and spread across multiple jurisdictions. Addressing these challenges requires broad-based domestic and international law enforcement cooperation, engagement with public and private sector organizations, and integrating new technical skills and tools with traditional policing methods.

Official statements by the RCMP and the preamble of the Convention highlights the fact that the Internet creates additional means to facilitate new and existing forms of deviancy and criminality. Each encourages greater transborder coordination for the state in attempt to (re)establish state presence online and to provide a degree of 'order' (perceived not to presently exist) within this additional, *cyber* environment that permits global interactivity.

In 2010, the Conservative Government forwarded the *Cyber Security Strategy* as a clear legal articulation to declare the executive's position on the international *Convention on Cybercrime* (2001) and one of the goals of the Royal Canadian Mounted Police:

> We are one of the non-European states that have signed the Council of Europe's *Convention on Cybercrime*, and the Government is preparing legislation to permit ratification of this treaty. Canada supports international efforts to develop and implement a global cyber governance regime that will enhance our security. To the extent possible, Canada will support efforts to build the cyber security capacity of less developed states and foreign partners. This will help forestall adversaries from exploiting weak links in global cyber defenses (Pubic Safety, *Cyber Security Strategy* 2010:8).

It is not hard to see how these statements may heighten privacy rights advocates' zealous concern toward these expanding investigative policing powers online. The "international efforts to develop and implement a global cyber governance regime" (ibid) may equally prompt some to believe Canadians are entering an era of persistent policing apparatuses and will also be subject to surveillance of other partner states within this 'global alliance'.

While an ominous depiction, it is perhaps indicative of impending measures yet to come, as *Convention* member states begin enacting lawful access into their own domestic law[16].

Despite any such positive intentions of the *Convention*, its legal force and effect have raised legitimate questions around the degradation of privacy online, rise of dragnet surveillance practices, increased information sharing agreements, as well as an absence of international human rights protection within online contexts. Others have also questioned if transborder cybersecurity harmonization will be of any value as some governments will be prone to cooperate with only those they share long and established historical alliances. Levin and Goodrick (2013) argue, "countries align themselves in cyberspace according to their geopolitical blocs, with several distinct cyber blocs having formed with their own unique cyber security strategies and emphases" (131)[17]. If state non-compliance transpires therefore among any member or signatories, information gaps will be perpetuated around "where [criminal and deviant] acts produce their effects" (ibid). Hence, governments will always have to accept the existence of a so-called "dark figure" of crime[18] (Skogan 1997).

---

[16] As Christopher Parsons (2012) observes, governments that have introduced lawful access legislation (e.g. U.S., U.K., Malta, India, France) have either expanded or have more broadly realized the powers they provide over time (i.e. misinterpreting the law). While I do not argue this will (deterministically) occur in Canada, the potential remains.

[17] International blocs may materialize among five regions: the *Anglosphere, European Union, Baltic, Commonwealth and Independent States* and *China*. Levin and Goodrick argue, "The barriers to effective cybersecurity are rooted not only in the technological composition of cyberspace but also in the political, cultural, societal and legal differences that hinder international cooperation in general" (129).

[18] In reference to crime, Skogan (1977) notes, "the problem is well known: an activity which is by some criteria a crime may occur without being registered in the systems devised to count it, thus reducing the accuracy of inferences from the data" (42). The RCMP (2014) also note, "Cybercrime is difficult to measure and often goes unreported to

Contemporary laws and policy prescriptions in the Asia-Pacific region indicates that many members do not entirely accept the particular notions stated above, as most are increasingly eager to be more familiar with what is 'out there' online and realize, "There is no turning back to a world without an Internet" (Public Safety 2010:14). Sections presented in the *Convention* are perceived to be a practical means for implementing crime reduction and crime prevention strategies, and perhaps for moving beyond the common rhetoric of "what works", which dominates not only a majority of policing and security studies literature (see Sherman 1986; Bayley 1998 and Jenion 2010), but also, the broader attitudes of 'civil society', governments, law enforcement and national security agencies when it comes to crime and its prevention or reduction.

In Canada, the reigning in lawful access legislation has been of interest for over a decade and a half. Lawful access' tenets directly ascend into Canadian propositions and a number of powers (i.e. tools and legal frameworks) deviate from original conceptions, as the technology that can be utilized and derived by law enforcement agencies outdates the original conceptions of this domestic cyber-crime framework proposal. The next section highlights a brief genealogy of lawful access within Canada, which is complemented by 'backstage' access to information records from a mosaic of GoC departments.

2.2.2 History of Lawful Access Legislation in Canada

Lawful access is predicated on providing Canadian police and national security agencies with extraordinary surveillance powers. Internal, 'backstage' RCMP documents (request #A-2011-06549), note that; "Lawful access consists of the lawful interception of

---

law enforcement agencies" (7). Moreover, as previously stated, cybercrime as a concept or potential object of analysis has lacked definitional clarity (see Valiquet 2011).

communications and the search and seizure of information used by law enforcement and national security agencies to conduct investigations and to gather intelligence" (5). While Canada's former Prime Minister Jean Chretien's Liberal government first conceptualized the idea of lawful access in March 1999 (Office of the Auditor General of Canada 2002), Canada's Liberal Party and Progressive Conservatives have each consistently ventured to establish its tenets into law during their respective times in office.

The first lawful access proposal was articulated in the Liberal Party's Bill C-74 on November 15, 2005, under former Prime Minister Paul Martin. Bill C-74 proposed that police need the ability to "listen to, record or acquire a communication" (RCMP request #A-2011-06549:1) absent of a warrant for subscriber data. However, on November 28th, a non-confidence vote was passed against Prime Minister Martin's government therefore failing to advance the bill beyond its first reading in the House of Commons.

On June 18, 2009, Stephen Harper's Conservative government introduced Bill C-46 and Bill C-47. C-47 proposed that TSPs must provide "the name, address, telephone number and electronic mail address…Internet protocol address [etc]" of subscribers upon receipt of a "written request" by any police service (10). Said differently, TSPs would be obliged to provide subscriber metadata telephony information upon a warrantless request. Indiscriminate collection of metadata without court oversight is a controversial notion, as it presupposes that the police had a right to access intimate, digital details of Canadians.

Accordingly, C-47 was vehemently opposed by legal critics, such as the Canadian Civil Liberties Association (CCLA) as well as Canada's former Privacy Commissioner, Jennifer Stoddart, who remarked that this Bill was a "serious step forward toward mass surveillance" (Raboy and Shtern 2010:191). Internal, 'backstage' RCMP records (request

#A-2011-06549) demonstrate that the government tried to dismiss these concerns. In one document entitled, "Setting the Record Straight on Bill C-47", the following news media line was carefully prepared for Harper: "Proposed legislation provides no new powers to intercept communications – police will still require a court order to intercept" (125). This narrative, however, is completely inaccurate and overlooked the fact that Bill C-47 would have allowed police to obtain subscriber metadata information absent of a warrant, which is information privacy experts consider to be even more illuminating than user-generated communications content (Schneier 2015; Privacy Commissioner 2014). This is due to the fact that user metadata illustrates patterns of movement, which are voluntarily produced when users explore the Internet but yet come to be automatically captured and retained by ISPs/TSPs. Meanwhile, the user-generated content is only as sensitive as one chooses: we choose what we post for others to view therefore giving users the ability to censor and to decide whether to participate. Meanwhile, online participation that generates metadata de facto can become a subject and artifact of observation, which may also carry insight for the police[19]. It is perhaps no surprise then that this media draft was never disclosed. C-47 also ignored the fact the Personal Information Protection and Electronic Documents Act (PIPEDA), has "allow[ed] TSPs to disclose to police…personal information about clients without their knowledge or consent and without any need for a warrant" (Bennett, Haggerty, Lyon and Steeves 2014:145). As Michael Geist (2014a:7) noted in Committee debates on the recent lawful access iteration (C-13), ISPs/TSPs often disclose "more than just basic subscriber information" when facilitated by PIPEDA, as its "so open-ended,

[19] This is of course in addition to the *social surveillance* users of social media conduct against one another. As Alice Marwick (2012) notes, social media websites are designed to "continually investigate digital traces left by the people they are connected to" (378).

content can also be disclosed voluntarily, as long as it does not involve interception…[its] by no means limited to basic subscriber information".

C-46 regarded the gathering of user tracking data and transmission data. Tracking data refers to "the location of a transaction, individual or thing" (Criminal Code, R.S.C., 1985, C-46, Section 492.1(8)); that is, electronic devices in possession of a person in the context of a criminal investigation (e.g. cell-phone or laptop). Transmission data regards the user metadata telephony information of an electronic device. Still, each of these bills failed to advance beyond Canada's House of Commons' Committee deliberation stage, as Stephen Harper asked the Governor-General at that time, Michaëlle Jean, to prorogue the Parliament in December 2009; that is, the second time the Conservatives shut down their government within a two-year period (the first being in December 2008) (Leblanc 2009).

Following these two failed attempts, the Conservatives then introduced three bills concurrently: C-52, C-51 and C-50. According to one 'backstage' Public Safety record (request #A-2012-00113), C-52 comprised of two, interrelated elements: mandate "TSPs to build and maintain intercept capable systems" and also "compel TSPs to release basic subscriber information" while requiring them to "remove any encryption" applied to user metadata (7). C-51 was proposed to ratify Canada's agreement to the Council of Europe's *Convention on Cybercrime* (2001). Meanwhile, C-50 offered to provide law enforcement with the "technical tools in order to investigate serious crime" and to also "permit the interception of private communications in exceptional circumstances", as one 'unofficial' RCMP record states (request #A-2011-06549:7). In an internal media document prepared for the former Public Safety Minister, Vic Toews, the Conservatives argued the combined "legislation is necessary to eliminate" the "safe havens" the Internet offers criminals and

terrorists (129); that is, C-50 would defer user anonymity online and "attempt to fill [a] legislative void" perceived to exist for Canadian police investigators (31). However, not one of these Bills prevailed, as the Conservatives were defeated by a non-confidence vote in the House of Commons, forcing a federal election later that year in May of 2011.

The 2011 election resulted in a Conservative-won minority government. Again, the Conservatives attempted to enact lawful access into Law. According to a 'backstage' RCMP document (request #A-2011-06549), this 'new' proposal was referred to as "Bill C-XX" (141) initially and later as, "The Modernizing Criminal Investigation Power Act" (155). As an 'unofficial' Department of Justice record (request #A-2013-00991) explains, "Bill C-XX (formerly Bills C-50, C-51, and 52) will equip police, CSIS and the Competition Bureau with the tools they need to ensure criminals and terrorist groups do not exploit technological innovations to hide their illegal activities" (58). Its elements were also considered "consistent with that of Australia, New Zealand, United Kingdom, United States" (59). In other words, it was parallel to the *Five Eyes* intelligence alliance, which Canada is a partner. Ultimately, this Bill became known as C-30 or more formally as the *Protecting Children from Internet Predators Act*. Interestingly, as Bennett et. al (2014) argues, the Bill was "renamed at the last moment…even though the bill actually made no reference to child predators except in its title" (144).

C-30 was largely a repackaging of previously failed bills; accordingly its sections will not be outlined. It is however worth noting that Bill C-30 was ultimately abandoned by the Conservatives due to the controversial elements around warrantless surveillance. Former Justice Minister, Rob Nicholson, delivered the statement toward the public, 'front stage': "We will not be proceeding with Bill C-30 and any attempts that we will continue

to have to modernize the *Criminal Code* will not contain the measures contained in C-30" (Payton 2013:N.P.). Vic Toews (2012), however, made one last attempt to garner support of opponents and Canadians that did not support their Bill, suggesting one year earlier in the House of Commons to, "Either stand with us or with the child pornographers" (5196).

Vic Toews' comments not only polarized Canadians and de-fused party agenda; it garnered international attention, especially online. For instance, the hacktivist collective Anonymous assembled in offence to Toews' comments by berating his remarks on social media websites. Certain segments of the *hive* went so far as to empirically demonstrate the dangers of allowing governments or anyone to have warrantless access to private user data, of which Bill C-30 had proposed. In fact, Vic Toews' data double was obtained by a sect of Anonymous who revealed to Canadians that Toews had once had an extramarital affair with his secretary; even conceiving one child with her. Their purpose was clearly articulated in a video uploaded to YouTube: "Anonymous will not allow a politician who allows his citizens no secrets to have any secrets of his own" (N.P.). This act of cyber disobedience highlighted the fact that even if people have nothing to hide in terms of criminality, privacy should not be squandered away under the guise of national security or 'protecting' children. Said differently, Internet user's subscriber information—content and metadata—are so sensitive that it should only be subject to disclosure after judicial authorization has been applied and granted based on the most stringent legal thresholds[20].

Despite promise to Canadians that any future attempts to introduce lawful access "will not contain the measures contained in C-30" (Payton 2013:N.P), the Conservatives

---

[20] While the actions from this 'branch' of Anonymous support the idea that judicial authorization be required before obtaining user metadata information, this idea may not encapsulate the ethos of other divergent offshoots. Anonymous is remarkably protean.

introduced C-13 (the *Protecting Canadians from Online Crime Act*) or known informally as the 'Cyberbullying Bill' in 2012; that is, less than one year after the party promise was made. Yet this time, lawful access *did* receive royal assent due to a number of factors that had not previously culminated (e.g. holding a majority government). As MP Sean Casey (2013) argued in the House of Commons, Bill C-13 "contradicts" the former promise by Conservatives and contains "37 of the 47 clauses" from Bill C-30 (1446). To this effect, sections were added to C-13 regarding cyber-bullying. Although, this was only narrowly tailored toward the criminalization of non-consensual distribution of intimate images (i.e. 'nudies') and did not account for other forms of cyber-bullying, as it was deemed that the *Criminal Code* already comprised of Sections that could be interpreted and applied within the context of the Internet (e.g. defamation or uttering threats). The manufacturing of said discursive enactments that reified lawful access in Canada is a key focus of this study.

The following chapter introduces an existing body of policing and security studies literature to situate lawful access debates in regards to how it reflects particular shifts in enforcement practices, as the Government of Canada begins to 'welcome' the age of Big Data and proactive, intelligence-led policing models to 'secure' the cyber environment.

3 Theoretical Framework

This chapter presents a theoretical discussion around intelligence-led policing (ILP). Part of what I am contextualizing and hypothesizing is that the move toward lawful access, as a framework to govern the Internet, is a reflection of the broader shift from reactive and targeted forms of surveillance toward more dispersive, proactive and *data*-driven efforts. Theoretical perspectives of ILP are situated in security and policing studies literature to explicate the rise of Internet policing and electronic surveillance. Firstly, an overview of ILP's history and applications in the context of the Internet is presented. Next, I highlight ways that law enforcement and national security agencies 'welcomed' this general shift in the era of Big Data. Finally, I conclude by exploring potentialities and issues of this trend as, the Government of Canada (GoC) proceeds to implement and forward these strategies in effort to seek out deviant and criminal acts that manifest in cyberspace.

3.1 Intelligence-Led Policing: from Reactive to Proactive

There are practical, working definitions surrounding the concept of intelligence-led policing (ILP). In the broader academic community, it has been chronicled as a form of predictive policing as well as proactive crime fighting "guided by effective intelligence gathering and analysis—and it has the potential to be the most important law enforcement innovation of the twenty-first century" (Kelling and Bratton 2006:6). Among the policing communities, it is understood to comprise of the "central tenets of command and control, community policing, problem-oriented policing, and data analysis" (Guidetti and Martinelli 2009:N.P.). Its theoretical tenets now challenge the more traditionally reactive,

incident-driven policing model and instead it employs new "strategic, future-oriented and targeted" means (Maguire 2000:316) to prevent and reduce crime. In North America and Western Europe, *proactive* crime prevention has been the keystone for managing risk in the cyber environment (Convention on Cybercrime 2004) and has become a precursor to harm reduction offline, especially following the tragic events of 9/11.

Known also as intelligence-*driven* policing (IDP), ILP has been a part of Western policing lexicons since the early 1990s (Ratcliffe 2003:1). Its etiology originates from the United Kingdom, corresponding with widespread calls by their citizens "for police to be more effective and to be more cost-efficient" at that time (2). External drivers equally contributed to its practical development (Ratcliffe 2003). First, spreading of transnational organized criminal syndicates and greater global interconnectedness has encouraged law enforcement agencies to find new means to comprehend or respond to multifarious social transformations of the Digital Age. Secondly, a rise toward neoliberal[21] practices within governmental departments consequently subjected ministries to considerable pressure to make better use of existing resources as fiscally conservative initiatives mired budgetary growth (Ratcliffe 2012). These conditions gave rise to novel policing-security policies thus contributing to harmonization among other nation states and private industries where procedural tools and laws did not formerly reach. This is to say that the consequences of

[21] While the concept of 'neoliberalism' lacks definitional clarity and is most often used pejoratively, I refer to neoliberal practices in the sense that the Internet has produced "an age of greater complexity, uncertainty, and volatility" for law enforcement (Thorsen and Lie 2006:17). As Ian Loader (1999) has noted, "successive Conservative (or, more accurately, neoliberal governments)" push to "remake the police and thus rebuild its legitimacy" and to deliver "efficient, prompt, courteous, value-for-money, professional service to all its customers" via partnerships and activities like "intelligence-led policing" rather than "high profile but 'ineffective' strategies (such as beat patrolling)" (376-377).

certain criminal acts are understood to exist outside of the jurisdiction of the individual domestic law thereby encouraging stakeholders from various enterprises and countries to coordinate, as criminal acts can emanate from beyond their geographical constraints, thus prompting new networks to emerge to facilitate intelligence gathering and enforcement of malicious and illicit activity. As chapter two highlighted, Canada's lawful access' tenets were derived out of the Council of Europe's *Convention of Cybercrime* (2001), which is largely predicated on an idea that, "Criminals are increasingly located in places other than where their acts produce their effects[22]" (clause 1).

Globalization, increased mobility and technological advancements have therefore facilitated the requisite for new means to account for the changing landscape of crime. In Canada, ILP arose in "near parallel development and popularity" as it did in England and Wales (Deukmedjian and de Lint 2007:249). It gained its sustenance in the wake of other practical failures of comparable proactive and intelligence-led policing approaches de jour: community-oriented policing (COP) and problem-oriented policing (POP). This is to say policing has always depended on accurate and timely intelligence for non-reactive, incident-driven crimes albeit based on the aggregated matters highlighted by a particular community or by recurring problems. However, intelligence-led policing differs from the above approaches in that the police make an effort to *actively* seek out the problems in a community or within a specific environment (physical or digital) before it manifests (i.e. is committed) or before crime develops into a more severe, chronic or normalized activity (Carter and Carter 2009). Maguire and John (2006) argue ILP is similar to POP as they

[22] This quote has also been utilized verbatim by Canada's Department of Justice (DoJ) in their *Lawful Access – Consultation Document* (2015).

both "focus on removing the root cause of problems rather than constantly responding to individual incidents" (74). However, COP and POP approaches were largely ineffective for reducing crime and fear of crime victimization, while also being slow to be adopted in contrast to intelligence-led policing models (Ratcliffe and Guidetti 2007:110-111).

The popularity of ILP is credited to the period and locale that it emerged, where the 'standard model of policing' was predominantly perceived to be ineffective for crime reduction and for improving public safety. In England and Wales, for instance, Ratcliffe (2003) notes that the number of police-recorded criminal incidents had risen 74% percent from 1982 to 1992. Moreover, citizen's *fear* of crime victimization grew exponentially in the same timeframe (Hough and Mayhew 1985). Accordingly, United Kingdom policing commissions, such as the Audit Commission (1993), made strategic recommendations for police to adopt an 'intelligence-led' and "comprehensive, corporate approach to tackling crime" (Ratcliffe 2012:2). The critical role of proactive intelligence collection therefore came to be regarded as one of the most necessary components for implementing effective crime reduction strategies while balancing the public purse. Indeed, it is a model that has been adopted by most Western law enforcement agencies today.

The next considerable event to catalyze the value of ILP models was 9/11. Since then, there has been an acclaimed belief among nations that "threats must be countered and suppressed *before* they are imminent" (Gill 2006:44). Intelligence and the *access* to it came to be regarded as the most conducive component for police agencies to thwart any potential attacks. As Willem de Lint (2006) cogently notes, "Intelligence is very topical. This popularization belongs most recently in the shadow cast by 9/11" (1). This is visible in the rise of multicolored policing agencies, which have now emerged across the world

to counter serious threats, which range from specific terrorist groups to broader actions of multi-issue extremists (or MIEs). For instance, within Canada, the Department of Public Safety (2014:N.P.) was created to help "keep Canadians safe from a range of risks such as natural disasters, crime and terrorism" by helping to coordinate various domestic and international policing partners. The basic notion was to network policing partners in order to improve information-sharing practices. New laws have equally kept pace; legitimizing and sanctioning policing, surveillance and security changes, but transformations have not always evolved at the speed desired by government. As chapter two illustrated, previous lawful access proposals set out numerous additional law enforcement tools, which would have allowed police to proactively gather bulk intelligence on Canadians (e.g. real-time metadata capturing or warrantless surveillance). Fortunately, such abundantly contentious elements never came into effect. Nevertheless, recent policy enactments such as Bill C-51 (known informally as the *Anti-Terror Act)* have further exacerbated privacy concerns by facilitating extraordinary powers to policing agencies absent of additional oversight[23].

Following 9/11, ILP has no doubt been "furthered by a number of federal public policy initiatives" in Canada and abroad (Carter and Carter 2009). Today, it has become the dominant framework for policing, especially as nations witness a rise in sophisticated criminal networks and threats redolent to the Digital Age (i.e. new ways to commit crime through the Internet). As Castells (1996:21) argues, we are said to be living in an *Age of Information* or rather an *Information Society*, where we value the role of information and technology. Reliance on computers is also "fundamentally altering the way we are born,

[23] Craig Forcese and Kent Roach (2015) discuss the false promise of security delivered by Bill C-51 in *False Security: The Radicalization of Canadian Anti-Terrorism.*

we live, we learn, we work, we produce, we consume, we dream, we fight, or we die" (33). To this degree, the GoC has urged for nearly two decades that policing technologies of power (i.e. laws and policing tools) must keep pace with the rapidly emerging changes of computing technology. On the other hand, few calls are made for more oversight.

Despite the fact that 'Internet policing' and cyber-security from the perspective of the GoC (2010) has been regarded as "the appropriate level of response and/or mitigation measures" contingent on the "severity of [a] cyber attack"—which Levin and Goodrick (2013) note is *reactionary*—the tenets surrounding lawful access are more indicative of being a reflection of intelligence-led policing paradigms. As the Director of Operations to the Ontario Provincial Police (OPP), Carson Pardy (2014) argued in House of Commons Committee debates, lawful access "takes [an] intelligence-led, integrated approach with our partners in policing and continued advocacy for the legislative tools needed to meet the law enforcement challenges of today" (5). Moreover, as Peter MacKay (2013) argued in earlier debates on lawful access in Canada's House of Commons, "The bill is all about updating offences to make sure that *any* prohibited conduct done through *any* form of telecommunication would be captured" (emphasis added, 1437). In other public debates, MacKay (2014) had also noted, "The portion of the bill that we are bringing forward are consistent, related, and support the common objective to give police the ability to *prevent* online criminal acts" (emphasis added, 8113). MP Mike Wallace equally supported the notion that, "C-13 would give police better tools to track and trace telecommunications" (8120). Meanwhile, MP Wilks (2014) argued lawful access is "a huge opportunity for the police to actively investigate something more *proactively*" (emphasis added, 4619).

Given the large quantity of data produced and captured in every day professional and social practices using technology, there is no doubt that ILP, while being regarded as a practical "business model" to carry out the "business of policing" *offline* (Ratcliffe and Guidetti 2007:111) has additionally become a useful framework to understand and situate present shifts toward lawful access and other modern electronic surveillance practices. As more regular criminal occurrences and rarities (e.g. terrorism) are speculated to increase in presence or to be represented online (Public Safety Canada 2010), the GoC has sought to secure the cyber environment and establish such an Internet governance model that has been perceived to be conducive for facilitating more proactive surveillance and to serve a greater crime prevention function. Yet, to date, other scholars have neither situated lawful access debates by drawing upon an ILP framework nor do others discuss how ILP models are emerging within the context of 'securing' Canada's cyber environment.

In summary, intelligence-led policing has become an organizational pillar for law enforcement in Canada (Brodeur and Dupont 2006) and has significant potential to thrive for policing as society depends ever more on the Internet for pleasure and vocation. ILP promotes the employment of intelligence to better comprehend and to act in response to emerging or (re)occurring "problems or risks" in society (Maguire 2000:316). In theory, this policing approach can provide law enforcement and national security agencies with better evidence (Ratcliffe 2002:63) to engage in targeting and surveillance of persistent or chronic offenders rather than focusing on more specific criminal incidents (Gill 2006:42). Extensive literature in criminology has affirmed the significance of focusing on such an offending population, as large fractions of offences are carried out by a small, committed number of offenders (Moffitt 1993; Farrington and West 1993).

In an ever more networked society, where data generation seems to be ubiquitous and theoretically amassable, it is no surprise that police have begun to adopt or to modify ILP models within the context of the Web. This is due in part to the fact that police can capitalize on the data-driven character—which defines many aspects of our contemporary society—for the purposes of collecting information, targeting certain person(s) or groups, and improving financial or analytical resources allocation to therefore disrupt more broad criminal markets or singular criminal incidents (Gill 2006:42). Policing—done digitally—reflects a move away from the *policing* of chronic offenders or person(s) of interests—of which ILP literature is traditionally concerned—and has instead become more focused on analyzing the *electronic patterns* of online user behaviour in the context of lawful access. Today, law enforcements' access to user's metadata telephony information appears to be both the site for the most promising way forward to facilitate proactive crime prevention online and yet has also subtly shifted law enforcement's focus toward different offenders through the unrestrained access to intimate, timely intelligence that could only be derived via corporate-led telecommunication carriers that host user data and individual actors (i.e. users) that generate troves of electronic data through multiple activities of every day life.

3.2 Policing Developments in the 21st Century

Information and communication technologies (ICTs) provide us countless tools to enhance a multifarious range of social practices. They permit social relations to extend to a new virtual realm allowing us to connect across both time and space (Wellman 2001). The Internet has equally dissolved national boundaries and evolved at high-speeds, which is often outpacing the legal systems ability to keep pace and to respond with conventional

procedural mechanisms. Given the Internet's boundless reach, the Government of Canada has searched for new technologies of power to respond to these present circumstances.

The abundantly complex architectural nature of the information superhighway has presented considerable challenge to law enforcement agencies. By its decentralized form, it contests the often bureaucratic and highly centralized structures of traditional policing units and of government more generally. In an era characterized by asymmetric[24] conflict and warfare, states 'welcome' new means of policing and new conditions of possibility to help govern crime, terrorism and every day deviant activity (Malone and Malone 2013). As the Internet becomes a 'Third space' beyond physical geographic boundaries of public and private life offline (Wall and Williams 2007), the Internet also becomes an additional "target of police action" and complementary space to govern people (Murphy 2007:468).

Over the past two decades, two significant developments have formatted policing practices: the growing dependence on notions of *information* and *networks* (Brodeur and Dupont 2006). Information relates to the usage of *data*, *intelligence*, and *data mining* for policing purposes in lieu of concepts such as *problem solving* in the community-oriented policing periods (see Deukmedjian and de Lint 2007:250). Networks refers to *networked policing* as previously state-driven activities are being delegated ever more to the private sectors; that is, divesting state responsibilities through multi-agency partners. Indeed, as

---

[24] As Josh Corman and Jericho (2013) argue, the Internet allows for a "low cost of entry [for] non-state actors to pursue war within cyberspace with great effect. Cyberspace gives minor actors global reach and impact. Hitherto, guerrilla war could only be fought successfully on one's home territory, as it was necessary to rely on the local population for support and anonymity. With cyberspace, it is now possible to project guerrilla war beyond one's home territory. It is now possible to gather supporters linked not by geography, but ideology" (83). Accordingly, the Internet supports decentralized, peripatetic and fractured means to conduct a myriad of legal and illegal activities.

Weimann (2004) notes, entire industries have emerged by problematizing the Internet and private sectors have stood to benefit from the 'problems' of the digital age. These trends have culminated to enroll private actors evermore within the production of security in the online context; this is most notably a trend that we have equally seen offline with private security firms taken up the former role of a government and citizens within communities for establishing or maintaining social control (see Statistics Canada 2009).

Bayley and Shearing (2001:5) have demonstrated there is an established history of "multilateralization in the governance of security". Governing[25] *through* and openly *with* other intermediaries was perhaps first observed in large measure with the configuration of the *Five Eyes* intelligence alliance[26], as allies committed to intercepting communications and electronic signals of Eastern blocs formed the alliance following World War II. Their purpose was to gather intelligence and to capture private cables and military strategies.

The *Five Eyes* set high precedent for intelligence collection and for policing. The *Five Eyes* presupposed that by harmonizing security efforts—each collecting and sharing data around communications or electronic signals—adversaries and/or multi-dimensional attacks could be detected and/or thwarted if rigorous surveillance systems were in place. Still, historical evidence of policing following non-wartime periods demonstrates that the police seldom use proactive means to reduce crime, prevent crime and to keep watch (see

---

[25] 'Governing' or 'governance' refers to 'policing', which as Brodeur (2007:26) notes, these terms were originally synonymous. This conception draws from the work of Dr. Johnson (1809) where 'police' was understood to mean "regulation and government of a city or country, so far as regards the inhabitants" (ii, police). In this sense, I refer here to novel means of policing Internet users and (consumers of) technology more broadly.
[26] Consisting of the USA, UK, New Zealand, Australia and Canada.

Maguire 2000). Policing has been dominated by reactive practices writ large. Still, it can be discerned that present electronic surveillance initiatives reflect these earlier ideals.

As Jenion (2010) comments, calls for proactive policing (prevention) can also be traced to 1965 in the United Kingdom with the Home Secretary's Cornish Committee on the Prevention and Detection of Crime. Specifically, Jenion has noted that the Committee made two recommendations: 1) establish specialized policing experts "whose sole focus would be crime prevention", and 2) "build relationships with organizations outside of the police who could be involved with crime prevention efforts" (36-37). After the disastrous event of September 11, 2011 (or 9/11), many of the concepts and practices established by the *Five Eyes* and declared in studies, such as the Cornish Report, gained (new) traction.

Following 9/11, there were powerful sentiments across countries to develop novel intelligence cultures and techniques of surveillance to shed light on the circumstances and causes surrounding the attacks (see Lyon 2003). Aspirations of using proactive responses to emerging and (re)occurring "problems and risks" became a derived necessity based on circumstances [and fear] at the time (Maguire 2000:316). One notable similarity to earlier forms of intelligence collection during the early years of the *Five Eyes* and the present is the reliance of the state on the private sectors for producing the technologies necessary to facilitate surveillance. A difference between then and now is that most of what we do in society (e.g. business and socialization) requires Internet connectivity and our movement *through* private sectors to facilitate daily activities. On one hand, it is therefore both the responsibility and choice of private entities whether they actively agree to be part of this modern 'surveillant assemblage' (Haggerty and Ericson 2000). On the other hand, recent revelations indicate deliberate state-sponsored hacking incidents where various security

intelligence agencies have implemented backdoors into the servers of corporate industries seemingly absent of anyone's knowledge or authorization (see Greenwald 2014). Global domestication and the reliance toward ICTs have no doubt fueled many of these so-called 'securitization' advancements in regards to lawful access. The data private industries are keepers to have therefore facilitated new, complementary forms to police and keep watch.

ICTs and the Internet therefore become both a source of intelligence and space for new problematizations of offending and deviancy. Murphy (2007) comments that ILP's "rhetorical value resonates powerfully in this age of insecurity, and validates the trend to broader domestic [and foreign] intelligence-gathering and analysis" (468). Further, ILP's philosophical and conceptual underpinnings are understood through "different definitions of different forms" therefore being malleable and open to new applications (McGarrel et al. 2007:153). Given intelligence-led policing is predicated on an idea of "broad levels of analysis of current and emerging threats (strategic intelligence) and more case-specific intelligence on individuals and groups believed to be actively involved in criminal activity (tactical intelligence)" (143), the Government of Canada has adopted many of these practices to help police and to keep watch. It is therefore framed here that Canadian law enforcement agencies have taken up an intelligence-led policing approach via novel surveillance paradigms that are dependent on accessing user metadata to not only manage crime and deviancy but to actually *preempt* crime's manifestation be it online or offline. Intelligence-led policing is equated therefore with quantifiable data collection rather than a synthesis or effective understanding on how to use metadata and without due care of the data quality objectives presented within a so-called 'liberal' democratic societal lens.

These security policy shifts have been legitimized principally due to the advent of lawful access legislation (i.e. Bill C-13) and external pressures to bring forward Canadian legal frameworks on par with their international policing partners (e.g. with the *European Convention on Cyber-Crime* where Canada is an official signatory state). Despite Bill C-13's royal assent in December of 2014, Canadian law enforcement and national security agencies have adopted intelligence-led policing models as a tool of governing *via* private

intermediaries (e.g. ISPs/TSPs) and also other sophisticated digital technologies for some time, as chapter five will highlight. Still, seldom have these trends been studied in detail to explicate the salient difference around why, how and to what extent this has arisen or how these trends impact state-endowed rights of privacy for Canadians. Specifically, no one has empirically argued that lawful access legitimizes policing aspects of surveillance already occurring, which previously contravened Canadian law before it came into effect.

3.3 Revisiting Surveillance: 'Welcoming' Big Data

Since 9/11, policing and surveillance trends evolved from the more conventional techniques facilitated by human-actor intermediaries as non-human actors (e.g. Big Data) present new potentialities for policing. While human-driven intelligence is still argued to be the "primary tool of high policing" offline (Brodeur 2007:35); ICTs now play a more integral, complementing component toward the alterity human actor. This is attributed to the extent that ICTs mediate evermore-significant portions of every day life. Beyond this, where surveillance and policing has predominantly hitherto been an investigation activity conducted *by* government(s) against citizens, corporations or other entities, in the context of the Internet, surveillance is delivered by the TSPs/ISPs while being entrusted to deliver paying subscriber's movement online. The trend toward private policing speaks generally to the 'pluralization' of policing and the rise of private sectors acting as an intermediary for carrying out activities, which have traditionally been left to a government offline (see Shearing and Stenning 1987; Jones and Newborn 1998, 2006; Button 2012).

Traditionally, surveillance in both policing and security studies literature has been understood to largely consist of "targeted scrutiny of populations and individuals" (Lyon 2014:2). It is regarded as a specific means to prevent harm, in theory and in practice, by

documenting the activities of very particular person(s) of interest. It presupposes that the act of surveillance is an invasive yet necessary measure to gather evidence for conviction or to help deter perceived harmful acts hypothesized to occur and/or remain undetectable otherwise in the absence of such conditions (Gillis 1989). In legal terms, it is legitimized under the auspices of the state that such an invasion and deferral of rights and freedoms (e.g. privacy) are demonstrably justified if the actions may ultimately benefit the greater good[27]. As Joh (2014) has contended, "While surveillance has long been an essential tool of the police, what has changed is its supporting technology" (48). Andrejevic and Gates (2014:185) note we can now witness a *double image* of surveillance emerge due to these shifts. The "familiar 'legacy' version of targeted, purposeful spying" continues to exist, but an "emerging model of ubiquitous, opportunistic data capture" has gained notoriety. This occurs not only in policing and surveillance; it is becoming more common among other sectors such as corporate campaigns, public health, transportation management, and advertising and marketing (see Bennett 2001; Duhigg 2012; and Tufekci 2014).

Contemporary efforts to keep records and to survey populations are nothing new. Take for instance the despotic regime of Nazi German Gestapo—a secret police agency once described as having the world's best "spy system" by the *New York Times* (Loughlin 2011)—who surreptitiously gathered information on vast populations. Their resolve was to identify persons considered a threat to the German Reich. Compare their efforts to the potentialities of technology in contemporary society and a much different picture begins

---

[27] This basic legal assumption is represented in many ways in Canadian law. Section 1 of the *Canadian Charter of Rights and Freedoms* for instance notes: the Charter "guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".

to emerge. Modern efforts require less human exertion, are often less costly and can also transcend outside of one's awareness (see Soghoian 2012:2). Whereas previous means for keeping watch would have allowed citizens to potentially 'see' surveillance efforts take place (e.g. with officers patrolling the 'beat'), modern technology acts as an intermediary preventing us from seeing the gaze of corporate or state surveillance. To this end, it has been said that keeping watch on the Internet is undoubtedly invisible in the Foucauldian (1991) sense, which is no doubt an exhausted metaphor in surveillance studies, as Dupont (2008) has noted. However, we can also understand and study these trends through highly publicized leaks, critical journalistic reporting, as well as academic research to help raise public awareness to these multiple and compounding effects. Still, electronic surveillance practices are no doubt disconnected from our perceptions or rather physical 'senses', as compared to the offline world. The public has to be *told* that it is taking place and *shown* evidence through some intermediary (e.g. the media); otherwise there is only speculation.

This is to say that the actions of today are predominantly automated and therefore transcend *through* technology. Indeed, such broad, totalitarian surveillance systems have existed before despite the access to ICTs and modern potentialities and reliance toward multiple private sectors for facilitating this process. Citizens are therefore not privileged to witnessing contemporary technologically-driven surveillance efforts take place. It is an automated, derived effect of ICTs we use in every day life and a consequence of existing in a more technology-mediated society[28]. Said elsewhere, characteristics of this type have

[28] As Warner (2012) notes, computers requires data 'spillage' to facilitate interactions. Without this communication (e.g. sharing routing address information, IPs, etc.) there are otherwise few means to navigate virtual spaces. One problem with this requisite structure is "voluntary disclosure of personal data", which is "written into the incomprehensible,

been conceptualized as a type of *high policing* (Brodeur 2007), "policing agencies collate data, process them into intelligence (analyzed information) and threat assessments, disseminate their intelligence products on a need-to-know basis, store them in various formats for a time and finally dispose of them when they have lost their relevance" (27).

These shifts have generated proactive data collection and analysis (i.e. *Big Data surveillance*). Mayer-Schoenberger and Cukier (2013) argue this shift has emerged due to persistent 'datafication' of the social world. Van Dijck (2014:198) operationalizes this as the "transformation of social action into online quantified data, thus allowing for real-time tracking and predictive analysis". Emergence of Big Data surveillance is indicative of what others term "dataveillance" (Clarke 1988), which is understood to consist of bulk collection and the analysis of information (e.g. metadata) through automated technologies controlled (i.e. owned) by sovereign bodies (most notably corporate) in perpetuity.

3.3.1 The Role of Metadata

As Andrejevic and Gates (2014:191) note but do not necessarily expound on, this new insurrection of Big Data surveillance has been supported by the sovereignty of ICTs mediated by the Internet in particular. The majority of persons utilizing and depending on Internet or other technology-driven processes exchange individual privacy for a reward of access and privilege. The cultural and socially entrenched trade of privacy-for-access has become so pervasive, stable and perpetual that consumers of technologies do not question or challenge their unnatural presence in every day life. Privacy within the digital sphere is

---

small type 'privacy policies' that people agree to daily" has now become "a condition of participation in the online economy" (Andrejevic and Gates 2014:191). In this sense, "This regime is supported and commensurate with a normalized and permanent 'state of exception,' in which individual legal rights are always suspended in any case" (ibid).

a fleeting commodity and endangered human right. David Berry (2012) proclaims, "Code and software become the conditions of possibility for human living, crucially becoming computational ecologies, which we inhabit with the non-human actors" (379). Code and software "structure[s] many of the life, memory and biopolitical systems and industries of contemporary society" (392) in both overt and covert forms albeit passively, aggressively and/or passive-aggressively. Technological participation therefore requires users to abide by certain structural rules (e.g. deferring privacy) in exchange for using services within a broader "regime of compulsory self-disclosure" (Andrejevic and Gates 2014:191), which is normalized in daily practices and has indeed become required to exist or to participate in multiple aspects of our personal relationships, parts of vocations and hidden pleasures.

To this degree, *life* becomes mediated by private entities capturing and storing our every virtual moments within a state of perpetuity. This is predominantly reflected in user *metadata*, which is often referred to as 'data about data'. Metadata shows *what* websites we connect to, *who* we connect with, *how* we connect, *when* we connect, and in particular ways, *why* we connect. As Michael Spratt (2014:4) noted in Committee debates on lawful access, metadata certainly "contains a great deal of personal information. It's a misnomer to simply call it metadata. That dilutes the importance and impact of that data". Questions of metadata and privacy have therefore been subject to examination in Canadian courts.

In the recent case of *R. v. Vu* [SCC:2013] involving the inappropriate search and seizure of two laptops and a cell-phone of a suspect, the judges noted in their final dissent in regard to Internet browsers and ICTs generally, they are "programmed to automatically retain information…[and] can help a user trace his or her cybernetic steps" (paragraph

42). Metadata therefore presents unique opportunities for policing and national security agencies. In the case of *R. v. Vu*, Canadian Supreme Court judges therefore dissented,

> In the context of a criminal investigation, however, [metadata] can enable investigators to access intimate details about a user's interests, habits, and identity, drawing on a record that the user created unwittingly…This kind of information has no analogue in the physical world in which other types of receptacles are found (ibid).

Concluding then, "privacy interests in computers are different–markedly so–from privacy interests in other receptacles that are typically found in a place for which a search may be authorized" (paragraph 47). This case forwarded the fact that police must obtain judicial authorization (i.e. a warrant) to search computer contents of a suspected offender[29]. Concerning, though, is the routine and (now) legal access that enforcement agencies have around procuring user metadata telephony information, as lawful access has set forward a number of sections that may further expand user electronic surveillance. The issue here is that while users abide to some exceptions to derive benefit or utilize particular digital services, such 'exceptions' (e.g. deferral of privacy) are extended to the gaze of the state; however, users are rarely notified or even aware that such surveillance activities are taking place or that they are ever subject to surveillance observations, as there are legal statutes in Canada to prevent user awareness of such tenebrous acts[30] (to be elaborated on further in chapter five).

Van Dijck (2014) notes in contemporary society, "Metadata in exchange for communication services has become the norm…the currency used to pay for online

---

[29] In *R. v. Fearon* [SCC:2014] precedent was set allowing the police to search a suspect's cellphone absent of a warrant following an arrest; even without recommending a criminal code offence. This raises questions of what *constitutes* a computer under Canadian law.
[30] See S. 7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act*.

services and for security has turned metadata into a kind of invisible asset, processed mostly separate from its original context and outside of people's awareness" (200). Soghoian (2012) notes users are provided access to a myriad of online services that seldom require financial cost; the 'cost' for participating in the digital sphere is "personal data"[31] (1). As a classified, backstage CSIS (request #A-2013-133) record remarks on the topic of metadata, "when you access the Internet you leave traces (history files, favorites, cookies)" (10) due to the perpetual capture of metadata by corporation, websites, TSP/ISPs and the Internet's default long-term retention of telephony information (16). This is to say activities that users engage in electronically are programmed to retain their information for extended periods. This fact therefore presents considerable opportunity for police to repurpose the data and construct profiles of individual habits, movements or choices. Police may therefore sift through the troves of metadata available by searching for particular 'keywords', websites visited or foreign and domestic Internet protocol (IP) addresses that can be regarded as being 'of interest' for national security or political, partisan contexts[32].

---

[31] Digital clients exchange privacy for access. Canadian federal employees now exchange biometric data (e.g. fingerprints) for employment as of Canada Day 2015. Examples of such exchanges are countless but the critical question is whether the tradeoff is justified.

[32] As one top-secret document in possession of CSEC (request #A-2013-00125) notes, "In 2012, CSEC started using a new on-line secure system to process requests for and disclosures of CII" (2). Another top-secret CSEC record (request #A-2013-00016) on *Procedures for Metadata Analysis* notes, *CII* means Canadian identity information, that is "information that may be used to identity a Canadian person, organization or corporation, including, but not limited to, names, phone numbers, e-mail addresses, and passport numbers" (19). As this record notes, this system "is currently in use with GC clients and, starting in the coming fiscal year, CSEC intends to extend its use to other GC clients as well as to its second party partners in the U.S., U.K., Australia and New Zealand" (2). Accordingly, while keywords allow police to target or hone in on specific activities, other systems exist to reify personal identity information of Canadians.

Multi-agency policing demands compliance of private sectors to secure the cyber environment, as state-run ISPs are atypical. Metadata access is a precursor to preemptive and predictive intelligence-led actions. Given the desire of the police to detect deviant or criminal acts, three options exist: 1) voluntary disclosures, 2) judicial authorization (e.g. warrants) or 3) unlawful access via implementation of 'backdoors' allowing for discreet, unauthorized access. The latter of which, for instance, is now known to have occurred by CSEC, as leaks by Edward Snowden reveal that the agency had covertly exploited known weaknesses in cell phone applications and Internet browsers (see Gallagher 2015).

3.3.2 Proactive Strategies, Reactive Purposes

Unique to traditional theories and praxis of surveillance, "Big Data surveillance is speculative" as government or industries can "amass an archive that can be searched and sorted retrospectively" (Andrejevic and Gates 2014:187). As Joh (2014) has argued, this provides fodder for states and industries to observe multiple facets of every day life; that is, surveillance may soon comprise of N=all, as societies depend on technologies and the Internet (41). Kitchen (2011) argues that ICTs are increasingly pervasive in nature—we are subject to many more voluntary and involuntary forms of surveillance than before.

In Senate Committee debates on lawful access, Michael Geist (2014b), an Internet lawyer and professor, noted America's former National Security Agency (NSA) general counsel, Stewart Baker, had once argued, "Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't need content" (21:28). Meanwhile, Geist points out the fact that General Michael Hayden, former Director to the NSA and Central Intelligence Agency (CIA), admits, "We kill people based on metadata" (ibid). It is therefore disingenuous to conceptualize metadata as just 'data about data'; its

analogous to unique digital biological information. It is not simply decoupled information separate from the user; it qualifies activities outside of content generation. In the context of activities that depend on using ICTs, users may not always generate content but users do perpetually generate troves of metadata for each moment connected. However, there is ample evidence to suggest connectivity may not always even be a precursor to metadata production; ICTs can generate metadata even if electronic devices are turned off (Priest 2013). This startling revelation has prompted some users to remove physical components, which provide energy to connect (e.g. batteries) when sensitive information is discussed offline in order prevent these 'Orwellian' potentialities of surveillance (Greenwald 2014). As a prominent cryptographer and computer security researcher, Bruce Schneier (2014), has therefore poignantly concluded, "Metadata = surveillance" (N.P.).

Unlike traditional forms of policing and surveillance, which are often targeted and purposeful (Lyon 2014); purpose and targets are irrelevant in the context of intelligence-led policing that is reactive. It is an afterthought. Andrejevic and Gates (2014:190) posit,

> Big data surveillance is not about understanding the data, nor is it typically about explaining or understanding the world captured by that data—it is about intervening in that world based on patterns available only to those with access to the data and the processing power…In the big data world there is no functional distinction between targets and non-targets (suspects and non-suspects) when it comes to data collection: information about both groups is needed in order to excavate the salient differences between them.

Surveillance target(s) therefore change dramatically in comparison to previous forms of surveillance, now a "target becomes the hidden patterns in the data, rather than particular individuals or events" (ibid). Brodeur (2007) remarks that the appetite for data collection in this context is limitless (27). In contrast to previous ILP assemblages where disparate actors aggregate after a criminal event transcends, 'multilateralization' of public (police)

and private (ISP/TSP) sectors is a *proactive* endeavor and precursor, of which "benefit[s] government, corporations–-and sometimes citizens" (Lyon 2014:9). It may be argued that while intelligence-led policing is largely proactive, it requires our previous knowledge of a particular phenomenon of events to occur before law enforcement may then accurately deduce what a particular likelihood may be based on the prior knowledge and 'signs' that existed before an event(s) had materialized into being. In the context of ILP online, a law enforcement entity might access private user metadata before and/or after such (criminal) incidents occur or are hypothesized to occur based on an 'objective' figure (e.g. if a user is searching 'How to commit an X or Y crime') therefore allowing them to intervene. The *objective* of Big Data surveillance is to therefore generate wide dragnets that may support surveillance; that is, proactively setting up webbing to systematically capture everything in its path. Metadata capture is therefore a de facto process of ICTs and computer servers of an ISP. Police therefore only require the enrollment of other actors to derive benefit.

A major thorn to this entire process then is the fact metadata retention periods are contingent on ISPs/TSPs that provide access to the websites and 'places' one travels to on the Internet. To this end, police can obtain a longitudinal glimpse into some of the most intimate activities of every day life if data is retained for extended periods of time. There is no functional equivalent to this form of surveillance offline. To analogize: if someone were the subject of an investigation, a warrant would need to be produced after obtaining judicial authorization to search their premises to look for clues about what they have been doing, where an artifact may be hidden in regards to some suspected offence, or when the suspect may have been in a specific place at some point in time. If the search and seizure of materials from one's premise proved to be futile, police would need to obtain evidence

based perhaps on a verbal interrogation of a suspected person, other potential eyewitness testimony or some unforeseen artifact, which may present itself at any particular point in time. The difference between this process and contemporary forms of digital surveillance is that online activities and metadata can reveal basically everything one does involving ICTs coupled to an Internet connection (and sometimes that is not required, as discussed earlier). What is perhaps even more troublesome is the fact that electronic surveillance of user metadata in Canada has largely been taken up devoid of a warrant and absent of the public's awareness for over a decade. Chapter five highlights this issue using a case study of lawful access, drawing attention to the discursive enactments of Parliamentarians and other interveners who retroactively legalized this policing practice into Canadian law.

To summarize, Big Data surveillance is unique to traditional practices as there is no requisite need to integrate purpose(s) or target(s) within primary development stages. Instead, the ambition is to collect aggregated data points *en mass*, which can therefore be used for purposes at a later date. Still, at a given moment, there is a need to produce code to reflect bias(es), which can identify matters, person(s) or items of interest. Bias is used in predictive analytics to discriminate against items regarded to be of no value by interest groups. Without bias, data points in a model would be considered as "equally good" (van Otterlo 2014:260). Big Data surveillance as a quantitative methodology therefore requires a "qualitative interrogation to disprove clams that data patterns are 'natural' phenomena" (van Dijck 2014:202). Questions still remain: what are considered matters of interest to policing agencies? What data, if any, is omitted from analysis and why? What role does transparency play? And, what are the social, ethical and personal costs of these activities?

In democratic societies, it is assumed that an ostensible balance between national security interests and civil liberties of citizens be met in the course of introducing novel means to police and to keep watch (Carter and Carter 2009). Yet, most of these activities culminate behind closed doors; that is, in secrecy. For political reasons and due to some exemptions in the *Access to Information Act* that protect national security and policing practices (at times for legitimate reasons), the Canadian public is often unaware of how policing activities are carried out. This is particularly true in the context of the Web, as there is no functional equivalent in viewing a police officer walk the beat on a street and online. This condition presents considerable challenges to study other, unofficial version of events, but presents unique opportunities to develop 'thick descriptions' (Geertz 1973), which can be made via established yet seldom-used methods for social scientific inquiry.

The next chapter outlines the methodological approach of the case study, which explored the discursive formations within the Government of Canada surrounding lawful access from both 'front stage' and 'backstage' vantage points. It highlights present scope of intelligence-led policing and surveillance practices within Canada on one hand and the proactive, pervasive collection of Canadian metadata telephony information on the other.

4 Research Methodology

This thesis explores the (re)emergence of lawful access in Canada; that is, a recent security policy shift that (retroactively) legitimizes law enforcement activities. It presents 'official' and 'unofficial' discourses to ascertain whether this law does not impact state-endowed rights of Canadian privacy, as the Government of Canada (GoC) has assured.

The research examines the intersections of 1) literature on lawful access, Internet surveillance studies and Internet governance; and 2) literature on intelligence-led policing and Big Data surveillance practices. Sociologists and criminologists who study theories and applications of intelligence-led policing (ILP) have tended to focus presences of risk offline (Ratcliff 2002, 2012). This has been done at the expense of investigating evolving social constructions of threat (see Tsoukala 2008) and efforts of state and non-state actors who search for new legal mechanisms and procedural powers to *police* cyberspace. Given the global rise of Internet use and its boundless, transnational reach, ILP theories require additional study as we begin to witness the blurring of jurisdictional authority for various policing communities and state-driven "efforts to develop and implement a global cyber governance regime" for Western allies (Public Safety Canada 2010:8). There appears to be significant risk that ILP—due to its transnational focus and dependence on computing technologies—is transforming policing aspects of surveillance beyond traditional police mandates with few checks and balances to ensure that the erosion of Canadian privacy is not occurring within and outside of their jurisdiction(s) of authority.

4.1 Case Study Approach to Canada's Lawful Access Legislation

The case study approach was selected in order to explore emergence of the GoC's recently assented lawful access legislation (Bill C-13) and to detail a historical and more

nuanced understanding of this security policy development. This strategy was chosen to generate "concrete, practical, and context-dependent knowledge" (Flyvbjerg 2001:70) to explicate and provide general insights on emerging policing practices by focusing on the narratives that arose from the analysis. The strength of the case study approach is that it is predicated on a constructivist tradition, of which presupposes that the research claims are relative and reflects the researcher's positioned perspectives (Baxter and Jack 2008). This method is most often used to support research questions that are more so descriptive and exploratory in nature (see Hesse-Biber and Leavy 2011). The contribution to this extent is that this case considers why, how and to what extent the development of lawful access legislation emerges within "the context within which it is situated" and through "a variety of sources" it "illuminate[s] the case" at hand (Baxter and Jack 2008:556). Influenced by the work of Flyvberg (2001), I iterate his notion that case studies can produce "concrete, context-dependent knowledge" for policing aspects of surveillance rather than attempting to principally generate "predictive theories" (72) but generalizing as well "on the basis of a single case, and the case study may be central to scientific development" (77).

4.2 Selection of Sources and Data Collection

This thesis utilized a qualitative, multimethodological research approach based on the analysis of documentary data from a variety of sources. Given the general absence of inquiries around lawful access, data was derived from primary source documents where possible to enhance credibility of evidence by existing outside of the researcher in a non-interactive manner (Reinharz 1992). This research draws from two intersecting domains: 1) publicly available information from the Parliament of Canada's LEGISinfo tool, which provided transcripts of Bill C-13 as it moved from one legislative stage to the next; and 2)

internal government records generated by law enforcement and national security agencies around Bill C-13, obtained using Canada's federal *Access to Information Act*.

As previously mentioned in chapter one, multidimensional datasets allowed the research question to be explored via two complementary, intersecting vantage points. On one hand, 'official' front stage discourse was collected to represent one side of the story of lawful access. In summarizing the work of Burton and Carlen (1979), both Walby and Larsen (2012) argue that 'official' discourse means the government's "carefully prepared, managed, and articulated messages" (32) to the public. As Goffman (1959) suggests, the 'front stage' is redolent to a public performance of an actor (in this case the GoC) on a stage toward an audience (the public), where they suggest, "the character projected before them is all there is to the individual who acts out the projection" (31). The 'front stage' dataset included but was not limited to: public broadcast media communications, website information, House of Commons and Senate debates, and Committee hearings.

On the other hand, 'unofficial' backstage discourse was obtained after contacting individual departments for records generated from the 'inside'. Burton and Carlen (1979) argue, "the discursive problem of Official Discourse is that it cannot hold up a mirror of legitimation to its own unitary image without recognizing the Other (unofficial versions of the crisis) which made the official discourse necessary" (22). This dataset included but was not limited to: internal emails, PowerPoint decks, internal research papers as well as personal memos. Walby and Larsen (2012) argue 'backstage' data is the "unofficial texts that are never intended for public circulation" (33) and thus can "illuminate governmental agency activities better than reliance on official discourse or carefully managed stories that government agencies themselves release" (34). By triangulating datasets (see Green,

Caracelli and Graham 1989), multiple dimensions of lawful access were understood via distinct but complementary vignettes in a chronological fashion. This helped create new "'hick descriptions' (Geertz 1973) for the case study using an iterative analytical process by drawing on datasets concurrently, which generated three, intersecting themes (Baxter and Jack 2008:554). The next two subsections detail the data collection strategy.

4.2.1 Publicly Available Information

The primary phase of data collection took place in the summer of 2014. Publicly available documents were purposefully sampled from GoC agency websites of networked stakeholders involved in the advent of C-13 and Canadian Internet governance practices. Focus was delegated to departments that actively engaged as proponents for creating new security policy shifts, as manifested in remarks made in the House of Commons and other hearings. This included Public Safety (PS), Department of Justice (DoJ), Royal Canadian Mounted Police (RCMP), Canadian Security Intelligence Service (CSIS), CSEC, Shared Services Canada and the Department of National Defence (DoJ). Data collection from stakeholder websites provided details on annual reports, commentary, and backgrounders. This aggregated data was used to explicate carefully regulated 'front stage' discourses in regards to policing tools and Internet governance frameworks, and any additional analysis of (re)emerging cyber threat activities or communicated strategies of response. Taken cumulatively, datasets provided records (i.e. content objects containing data/information) (NISO 2010:4), illuminating a general understanding of agency perspectives on lawful access as portrayed via constructed information packages widely disseminated toward the public stage. Each record was read in its entirety to facilitate an open-data coding process without presupposing or creating focused searching entries to reduce deductions outside

of original contexts. This dataset served as a cornerstone to understand and contrast front stage displays against backstage data obtained using the *Access to Information Act*.

The second phase of data collection proceeded concurrently to the first, but yet it evolved into the latter part of fall 2014. This step involved the capturing of the legislative processes surrounding C-13 from its initial reading in Canada's House of Commons on November 20th, 2013 until it reached royal assent on December 9th, 2014. This dataset provided a thorough description of narratives around some of the public declarations for *why* the GoC introduced this framework and *how* its effectuation may impact Canadian privacy, as articulated by Parliamentarians, legal experts and public witnesses at stages of the legislative process. Data was collected using the GoC's open-access LEGISinfo tool, providing transcripts of legislative meeting minutes of Parliamentarians and interveners in an organized and systematic PDF-readable format. Data was examined in its entirety; that is, reading each line that captured every spoken word at each stage legislative stage. PDF-readability allowed keywords to be searched, which was critically once the thematic codes began to emerge, allowing a re-visitation of particular items of interest later on.

Table 4.2.1: Bill C-13 Status and Date

Status (Legislative Stage)	**Date (YYYY-MM-DD)**
First Reading (House of Commons)	2013-11-20
Second Reading (House of Commons)	2013-11-27 2013-11-28 2013-11-29 2014-04-28
Committee (Standing Committee on Justice and Human Rights)	2014-05-01 2014-05-06 2014-05-13 2014-05-15 2014-05-27 2014-05-29 2014-06-03

	2014-06-05 2014-06-10 2014-06-12 2014-06-13
Report Stage (House of Commons)	2014-09-22 2014-10-01
Third Reading (House of Commons)	2014-10-10 2014-10-20
First Reading (Senate)	2014-10-21
Second Reading (Senate)	2014-10-23 2014-11-05
Committee (Standing Senate Committee on Legal and Constitutional Affairs)	2014-11-05 2014-11-06 2014-11-19 2014-11-20 2014-11-26 2014-11-27
Third Reading (Senate)	2014-12-02 2014-12-03 2014-12-04
Royal Assent	2014-12-09

4.2.2 *Internal Government Records*

The third data collection phase involved the procurement of internal GoC records using Canada's federal *Access to Information Act*. To move beyond the public, 'official' discourse, journalists have frequently used this method of inquiry, but it has only recently entered scholarly query in the social sciences as a tool to complement the more traditional or 'established' methodological approaches (Gentile 2009; Piche 2012). With exceptions of clauses in the *Act*, which exempt disclosure of specific records, scholars consistently demonstrated its use for gaining 'partial entrance' (Walby and Larsen 2012:39) into the regulated 'backstage' activities of the state, which can be triangulated with other datasets.

In qualitative case studies, boundaries around the case support a critical role to define the scope and breadth of research projects (Baxter and Jack 2008). To establish what evidence was to be included and excluded from analysis, requests pertaining to the

following topics were sought after: lawful access (to situate current debates historically), Big Data surveillance (to help frame the analysis), records relating to the use of electronic surveillance by law enforcement as well as the role of metadata information for proactive, policing purposes. ATI requests were acquired from the following GoC stakeholders: PS, DoJ, RCMP, CSIS, Department of National Defence (or DND), CSEC, Industry Canada, and Security Intelligence Review Committee (SIRC). Taken cumulatively, these records provided an aperture into the daily, 'closed-door' practices to therefore illuminate "what the state says about its policies and practices" from behind the scenes (Piche 2012:235).

Despite a myriad of benefits that can be derived from using ATI request from the ability to generate what Gary Marx (1984) has called 'dirty data' to representing primary ("texts"), secondary ("work") and tertiary ("networks between organizations") levels of analysis (Walby and Larsen 2012:34), there are still a number of significant drawbacks. I highlight two in particular but there are numerous. For one, data produced is often subject to information exemptions thus—like social scientific inquiry—records are often "partial, incomplete and context bound" (Rallis and Rossman 2012:50). This is reflected to the extent that texts can be redacted through white spaced ('positive redaction') and/or black spaced ('negative redaction') arrangements (Larsen 2013). The former is problematic for comprehending text(s). As Larsen has noted, negative redaction removes content without permitting the viewer to realize whether a record under investigation is missing a "line, or a missing paragraph" or any other artifact, as the text is redacted using 'white spaces', of which predominantly rests in front of 'white backgrounds'. This is considered 'negative', as no method exists to elucidate the differences among the missing pieces of the puzzle.

On the other hand, black spaced redaction represents an "archetypical image" (39) conjured up when one hears the word 'redaction'; that is, text "crossed out with a black marker" (ibid). This approach is regarded to be 'positive' in the sense that it can provide researchers with an informed understanding of the pieces that are being withheld. This is due to the fact that the researcher can make out shapes and lines—discriminating against what is *likely* a paragraph, figure or operative word. Information redaction is intimately linked and inseparable from the concept of state secrecy and questions around whether the release of sensitive information may result in an injuries to national security, as a backstage classified Public Safety document notes (A-2012-01994:134). In regarding the analysis of internal backstage documents, an "informed reader"[33] may be able to come to conclusions that are "statements of the obvious" that can be tricky "to prove or disprove" (136; citing *R. v. Almalki*, 2010). Craig Forcese (2007) has referred to this process as the "mosaic effect", that is, a *knowledgeable reader* can potentially damage national security when the outcome of research results in the "mosaic of little pieces of benign information that cumulatively discloses matters of true national security significance" (55). While this research does not damage or cause any such injuries, it brings security intelligence and policing practices under question, which answers would no doubt benefit from a public response. As one internal Public Safety record notes, certain information discussed in this

[33] While the Canadian courts (see *Rajadurai. v. Canada* 2009), in the context of security intelligence practices and the duty of disclosure, define an "informed reader" as "a person who is both knowledgeable regarding security matters and is a member of or associated with a group which constitutes a threat or a potential threat to the security of Canada, will be quite familiar with the minute details of its organization and of the ramifications of its operations regarding which our security service might well be relatively uninformed" (135), I refer to it here as a researcher who has previous experience studying Canadian law enforcement and security intelligence practices using the *Access to Information Act*.

thesis places agencies in a "conundrum"; being unable to respond to my comments due to the limitations and sensitivity of their work, as articulated in the *Access to Information* and *Privacy Act*. However, given the general lack of openness and transparency among certain department practices under study, I agree as the internal Public Safety (A-2012-01994) record remarks (in citing *R. v. Almalki* 2010), "'information which might be clear and relevant if the full context were to be disclosed may become obscure, equivocal, and even misleading when a piece of the context is removed' by redaction" (136).

Secondly—or arguably the first—most prominent roadblock in using this research method is that agency disclosures take a significant amount of time to obtain; that is, time researchers are not always afforded. As Larsen and Walby (2012) note, requests can take the better part of several years to obtain depending on the scope of requests and potential barriers presented by the agency being *brokered* for access. That being said, this research uses formal and informal (i.e. previously competed) requests obtained in undergraduate and graduate study. This was purposefully done to ensure data was gathered in a manner to facilitate the timely completion of this project. Having engaged with Canada's *Access to Information* and *Privacy Act* for several years (thanks to introductions and teachings by Mike Larsen[34]), objects of study are arguably better understood when combined with accumulated records. This phase proceeded in an iterative process as analysis of requests provoked additional questions and channels for inquiry, present and future. Accordingly, supplementary requests were made and acquired into winter of 2015. The following table

[34] Those interested in ATI research are encouraged to read *Access in the Academy: Bringing ATI and FOI to academic research* (2013), which is freely available online.

highlights the individual request numbers obtained by a mosaic of departments involved in the lawful access surveillance context used for this study[35].

Table 4.2.2: Access to Information Requests by Government of Canada Department

Government of Canada Department	Request Number
Canadian Security Intelligence Service	A-2012-088 A-2012-168 A-2013-133 A-2012-248
Department of Industry	A-2013-00415 A-2012-00715
Department of Justice	A-2013-00991
Department of National Defence	A-2012-01145 A-2013-00723
Department of Public Safety	A-2012-00113 A-2012-00261 A-2012-00262 A-2012-00234 A-2012-00310 A-2012-01994
Royal Canadian Mounted Police	A-2011-06549
Security Intelligence Review Committee	A-2010-07
Shared Services Canada	A-2013-00991

4.3 Data Organization and Presentation

Data was compiled using the software ATLAS.ti 6. First, the non text-searchable records were treated through Prizmo's optical character rendition software program. This allowed documents (e.g. ATI records) to be viewed in a searchable format. Next, publicly available records—previously searchable—and internal GoC records were uploaded into ATLAS.ti 6 and coded according to thematic structure (Attride-Stirling 2001). ATLAS.ti 6 is frequently used in qualitative research and provides the ability to work closely with

[35] Summaries of requests can be obtained by inputting request numbers into the GoC's *Completed Access to Information Requests* portal at: http://open.canada.ca/en/search/ati. Note: not all ATI request numbers are publicly available via this portal due to a lack of database maintenance or poor departmental reporting; requests are also removed at times.

datasets simultaneously to create focused coding and open-data coding schemas (Strauss and Corbin 1990). Given the software's ease to facilitate text-based retrievers and code-based software, thematic codes were assigned to the emerging narratives. Variables were generated to group analogue content (e.g. comparing official and unofficial discourses) around particular cases, events and/or controversies. ATLAS.ti 6' systematic organization of datasets was critical to the timely completion of this research.

4.4 Research Process and Data Analysis Strategy

This study is principally concerned with the employment of *textual analysis* to explore the question of why, how and with what effect intelligence-led policing models are being adopted to 'secure' Canada's cyber environment. As Walby and Larsen (2012) remark, *text* is argued to be the most important element for the investigation of activities and internal processes of government. Although they have acknowledged texts "do not do anything by themselves" and they "need to be activated by government workers...penned or typed", when focusing on the element of text, this study adopts their notion that we can "take the work of government agency employees as an object of analysis" (34).

Given both the "partial, incomplete, and context bound" nature of social scientific inquiry (Rallis and Rossman 2012:50) and "partial entrance" to the state's backstage vis-à-vis access to information (Walby and Larsen 2012:39), triangulation was imperative for producing a holistic understanding of the case. As Hesse-Biber and Leavy (2011) explain, triangulation occurs when researchers employ two or more methods to study the research question (280). By drawing on a multimethodological approach, data was obtained from two sources, as described in previous sections, with distinct time intervals between each phase of the research process. This provided opportunity to be positioned and prepared

for how "information gleaned from one module of the data production can inform future data production efforts" and future research (Walby and Larsen 2012:39). Triangulation as a qualitative approach does not necessarily equate to "better research" projects, as Julia Brennan (2005:183) has argued; it allowed findings to be presented in a post-positivistic, phronetic research paradigm. In other words, it allowed for focus at the *actor* level using ATI records and Parliamentary transcripts while situating relations to a macro, *structural* level (e.g. Big Data surveillance) to make dualistic connections between these elements.

Given the emphasis on *text* and explorations of "implied meaning, argumentation strategies, the sources of knowledge, and agentive structures and symbols" (see Tenorio 2011:192), this research used discourse analysis to explore the productions of 'official' discourse in relation to what is excluded based on the evidence from 'unofficial' records. Hesse-Biber and Leavy (2011) argue discourse analysis is embedded in "postmodern and post-structural conceptualization [in] that language reflects power" (238). The discourses were explored through broader sociological questions around how lawful access had been constructed and problematized from 'front stage' and 'backstage' vantage points.

Discourse analysis as a methodological approach when combined with the other methods framed a more holistic and nuanced understanding of the case study. The use of discourse analysis was informed by theorizations of Walby and Larsen (2012), who argue that publicly available data and access to information records do not provide insight into the 'backstage' and 'front stage' on their own. Yet, when *combined* and "treated through discourse analysis" a more "complete picture" can begin to emerge (39).

Ultimately, a balance between two discursive approaches created the potential for creating thick descriptions around the case. By analyzing these datasets concurrently, the

"production of official discourse and changes in the production of discourse in the agency" were highlighted (Walby and Larsen 2012:38). This allowed the case study to be explored historically through "sequential and longitudinal design to explore the work of government agencies over time" (39) as documentary data spanned from January 1, 2008 to December 9, 2014. This approach was critical to explore the *why* and *how* components of the research question, as analysis of historical developments helped to contextualize the case and frame analysis, discussion and conclusions around *what effects* intelligence-led policing models may have on the lived reality and privacy of Canadians.

To frame the analytical technique of discourse analysis, I drew from the works of Normand Fairclough's (1989, 1995) methodology of *critical* discourse analysis (CDA). By employing CDA, attention was paid to 'social effects of texts', and how *texts* can be actors (Latour 1987, 2005); carrying potential to "bring about changes in our knowledge (we learn things from them), our beliefs, our attitudes, values and so forth" (Fairclough 2003:8). It thus presupposes the "social world is textually constructed" (9). In examining Fairclough's method, Janks (1997:330) has argued it is crucial to engage with texts via integrated approaches between the *engaged* and *estranged* position, noting, "The theory and practice of CDA suggests strategies which enable this deliberate move and argues the need for reading against the text to counterbalance reading with the text" (331).

Given that *critical* discourse analysis often "seeks to understand how discourse is implicated in relations of power", as Janks (336) has noted, I did not want to presuppose relationships of power, inequality or stratification to emerge from the research process *a priori*. Yet, I recognize that debates around lawful access has caused a (re)negotiation of powers for police and notions of Canadian privacy, as the GoC responds to (re)emerging

cyber threats. Accordingly, it is recognized that this reflects an exercise of elite, state and capital power (Mills 1956) as a means to confront issues at the forefront of cyberspace, as the Internet transcends and affects the offline domain.

In phronetic research, discourse analysis can be regarded as a "complete package" for social scientific inquiry using, as Jørgensen and Phillips (2002) note, "philosophical (ontological and epistemological) premises…theoretical models…methodological guidelines…[and] specific techniques for analysis" (3-4). It also encompasses degrees of flexibility, as researchers are not restrained from developing his or her "own package by combining elements from different discourse analytical perspective and, if appropriate, non-discourse analytical perspectives" to form "*multiperspectival* work" (4). As a result, I also drew on Laclau and Mouffe's (1985) discourse theory for their range of analytical focuses and ability to seek out interrelated focal points for discursive forms. Arguments by others note that their works, however, "do not supply concrete methods for analysis" (Jørgensen and Phillips 2002:165), thus their contributions were loosely engaged with to the extent that certain phenomenon become mediated through discourse by their effects.

Theoretically, this project seeks to evolve some conceptualizations of security and intelligence by building on the work of Walby and Larsen (2013) and Michael Geist. It seeks to offer new conceptualizations around intelligence-led policing, by contributing to the growing subfield of Internet surveillance studies. The core concepts that informed this project are intelligence, surveillance and law. These concepts reflect practices of police and security intelligence communities as well as the efforts for 'securitizing' the Internet. Still, there are without doubt limitations and implications to the chosen approach.

Given the nature of ATI records being part of public record and this thesis' open publication, Walby and Larsen (2012:40) have argued that researchers therefore become "open government activist(s)" by implication. If we accept their argument, the meaning making and interpretations might impact the ability to carry out future requests among the agencies examined. As Alasdair Roberts' (2002) employment of ATI in his research illustrates, departments routinely categorize and typologize requesters, which can impact the ability to obtain records in the future despite the equal access clauses embedded in the *Access to Information Act*. Piche (2012) remarks that various *techniques of opacity* also exist in this regard including but not limited to: postponing requests, declaring high cost or fee estimates for processing the request, and simply, non-acknowledgement of receipt that a request was ever made (245). In this vein, there are questions of whether this thesis may hinder future projects or prospective employment, given the ability for an agency to deem the project to be unflattering to some departments. Given the emphasis on access to information requests, there is potential for agencies studied here to also come across this project; this may present future opportunities to submit additional requests to agencies for evidence of this; though this may play well into the themes of this research: surveillance, metadata, policing.

Interviews with user stakeholders may have also complemented the analysis. Still, given the seldom access granted to researchers for the agencies under investigation, this method was only considered in passing. It is assumed that the datasets presented here are sufficient to generate empirically grounded analysis of the case study. Nevertheless, there is opportunity to build on premises here for future inquiry where an even longer period of research time can be afforded.

5 Re://Presenting Lawful Access

In previous chapters, I introduced existing scholarly debates around how issues of cybercrime and cyber-security have come to dominate much more discourse in the media, criminal justice system and Government of Canada (GoC) around public order. I also chronicled the (re)emergence of lawful access in Canada and exemplified how this policy directly descended from the *Convention of Cybercrime* (2001), which encouraged transnational harmonization for policing aspects of surveillance. Moreover, I presented a theoretical discussion around lawful access legislation; arguing that it is a reflection of an intelligence-led policing (ILP) paradigm evolving from offline schemas, targeting chronic offenders to online actions that encapsulate electronic (metadata) patterns of behavior to detect and prevent deviant and criminal acts, online and offline.

This chapter proceeds to present three, interrelated narratives surrounding lawful access in Canada at the intersections of policing, governance and 'Big Data' surveillance. Section 5.1 and 5.2 explores how lawful access gained support via discursive enactments on the 'front stage' in its foremost iteration and argues that the Government capitalized on recent tragedies of cyber-bullying to resurrect invasive policing aspects of surveillance from previously failed lawful access proposals. In section 5.3, I challenge the prevailing state assumptions, which presupposed lawful access is necessary to 'secure' cyberspace and that new legal frameworks were required for state and non-state actors. Specifically, I argue that lawful access was reified to retroactively legitimize previously occurring policing practices, which contravened Canadian law.

In subsection 5.3.1, I detail one (knowable) scope of state-directed surveillance taking place against Canadian citizens for non-criminal purposes and draw attention to

what I refer to as a *pay-per-view-disclosure* system where Canadian policing agencies pay TSPs/ISPs for metadata records of citizens. In section 5.4, I highlight the case of *R. v. Spencer* to engage in a discussion around the Supreme Court of Canada's qualification of privacy rights in the context of the Internet. I argue that while *R. v. Spencer* constitutes the unmistaken parameters around policing aspects of surveillance, issues of transparency and reporting remain in certain departments and TSPs/ISPs therefore preventing ability to appreciably understand whether the police and corporate entities are operating in a pre- or post-*Spencer* framework. In section 5.5 and related subsections, I conclude by presenting a discussion around the implications of these policing trends, arguing present surveillance trajectories have an ability to exacerbate a civil divide between citizens and government due to issues of distrust and potential 'fishing expeditions', which might indiscriminately target particular persons based not on so-called objective, empirically-based evidence but vis-à-vis policing and security intelligence frameworks that actively problematize aspects of the Internet. To this degree, I answer the following research question from front stage and backstage vantage points: *why, how and with what effect are intelligence-led policing models being adopted to secure the cyber environment?*

5.1 Manufacturing Support

Policy prescriptions regardless of their persuasion require their activation by some external figure or institution in a democratic society. It is not simply enough, lawful to do so or publicly acceptable (except under exigent circumstances), for governance structures within democratic confines to bring about policy measures absent of any legislative body, entered debate or without working through some established regulatory procedures. Open and transparent debate equally serves a critical function to maintain and to develop public

trust. Policy-making is a malleable event, neither deterministic in its consequences nor in its affect as it requires those legally empowered to use its powers to do just that. It is open to both known and unknown challenges, counter-balance and deactivation either at point of its departure or a later stage in its time.

Mitchell Sharp's (1969) discussions around the bureaucratic elite in the Canadian government and the construction of policy formations highlights the fact that the work of government is not "highly theoretical and divorced from the everyday world"—of which is perhaps more visible in 'academic' or 'ivory tower' thinking—governmental work is primarily concerned with one simple question: "will it work?" (85). Public servants try to activate these questions and to determine feasibility in the policy *making* stages whilst the elected representatives attempt to *reify* the policy by lobbying its tenets toward the bodies of the Cabinet and the House of Commons within the Canadian context (86).

When the newest lawful access legislation (Bill C-13) was forwarded to Canada's House of Commons, Peter MacKay (2013)—the Minister of Justice at the time—argued,

> We are trying to put police investigative powers in place on the Internet, where so much information, and therefore danger can exist. Unfortunately, technology moved at a much faster pace than the legislation that would enable police to do their job properly…we want to be able to give the police the power to do that, to protect children, protect information, protect finances and protect against terrorism. All of this is about giving police tools in the modern era (1440).

Statements and sentiments of this demeanor proceeded forward throughout official (front stage) and unofficial (backstage) discourse. Its therefore critical to interrogate the validity of these ontological claims, especially considering, as MP Sean Casey (2013) has noted, it was only one year prior to Bill C-13 that the former Justice Minister, Rob Nicholson, had adamantly stated: "[The Conservative Party of Canada] will not be proceeding with Bill

C-30 and any attempts that we will continue to have to modernize the Criminal Code will not contain the measures contained in C-30" (Payton 2013:N.P).

5.2 Framing Lawful Access as a 'Cyberbullying Bill'

Recently**,** stories of personal tragedies have played out in the lives of Canadians as a result of the mediating potentialities of technology, especially the Internet. A real and hypothesized effect of cyber-bullying has materialized in the consciousness of Canadians following the suicides of several youth: Amanda Todd and Rehtaeh Parsons. In House of Commons debates on lawful access, MP Francoise Boivin (2014) argued, "Bill C-13 was created in the wake of tragic situations involving certain Canadians" but while containing "47 clauses [and being] 53 pages long…it does not even touch on cyberbullying or online crime" (7656). To this degree, lawful access legislation is argued to be a reformulation of previous attempts in its fifth iteration to the tone of a particular and highly sensitive issue ignited within public consciousness. No doubt is the issue of cyber-bullying one that is deeply concerning and serious. Yet, an understanding of the history and the rise of lawful access law—as outlined in Chapter Two—demonstrates hitherto that cyber-bullying was never a prior caveat until its foremost iteration. Instead, it appears Government used the issue of cyber-bullying as a symbolic and empirical case to garner empathetic support and demonstrate state action while reigning in additional tenets of other previously failed Acts. For instance, one media line prepared by Canada's DOJ (request #A-2012-00991) for a theoretical 'Question and Answer' period on Bill C-30 (the predecessor to Bill C-13) presents a different understanding of the latest Bill introduced; making the official, front stage narrative to appear disingenuous to say the least:

> Question: 'Will the problem of cyber-bullying be addressed?' Answer: 'This Bill does not provide a tool uniquely for cyber-bullying. However the

> Criminal Code already contains a number of provisions that tackle criminal activities that may be relevant in cases of cyber-bullying. In particular, the offences of criminal harassment and uttering threats are available to deal with the most severe cases of cyber-bullying. This bill is focused on updating provisions to reflect modern communications, and this includes the provisions relating to false messages and indecent and harassing phone calls, in order to bring them up to speed with the Internet age. Updating the language of these existing provisions will ensure they continue to apply in the context of these crimes when they are committed using modern communications. This may, in some instances, be relevant for cyber-bullying' (24)[36].

Hier (2008) argues that expanded governmental (executive) power(s) and their legitimacy into law can often emerge via the moralization of some social issue and/or grievances that "call for action on the conduct of harmful others in an effort to eliminate some specific activity or behavior that has already occurred" (183). Said differently, creation of policy requires ignition of a moral panic(s) over some particular issue or concern (albeit social, economic, political, and/or cultural) in order to then generate the required support needed to therefore bring about measure(s) perceived necessary and/or of benefit to us all (Beck 1992). Rhetorical techniques that generated such a "panic" were represented throughout lawful access debates at various legislative stages to the extent of problematizing cyber-

---

[36] Prepared 'Question and Answer' in Government is perhaps indicative of broader trends between Stephen Harper and the media. Since April 2006, Harper has seldom answered a question posed that he was not previously privy to receiving beforehand. This is due to his idea that, "The press gallery has taken the view they are going to be the opposition to the government" (Hennessy 2011:51). As Hennessy notes, his Government has chilled freedom of speech and critical reporting by using a "central list where reporters [are] forced to sign up in order to have a chance of covering a PMO story" (50). Further, "The government has framed the issue as trying to bring 'order' to a practice that is 'chaotic' and an institution that is outdated…Control and secrecy are the waters that Harper swims in" (51). While the rehearsal of carefully managed 'Questions and Answers' is expected for organizations and actors held to their public displays, it appears information control or message discipline is one that stems from the 'backstage' to the 'front stage' and likely across other GoC departments. However, as Taras has argued, "You can only control events for so long, you can only manipulate for so long" (as cited in Hennessy 2011:53).

bullying as a looming social problem that could deliver harm to any Canadian thereby requiring expansion of state powers and 'new' legal frameworks for departments, private industries as well as policing and intelligence communities.

As MP John Carmichael (2013) argued in House of Commons debates, "This bill brings hope to all Canadians. It brings us an opportunity to put regulation and legislation in place that will protect our children and our grandchildren from those who would take advantage of them" (1516). Notions of 'hope' and arguments around 'opportunity to put regulation and legislation in place' under the very auspices of protecting Canadians helps connect symbolic and discursive transformations through meaning making. It establishes a 'means-goal' (see Fairclough and Fairclough 2012) to the extent that it presupposes that a specific state response (e.g. establishing lawful access) will provide 'security' for future generations to come. In doing so, rhetoric is supported by premises of 'hope' and through persuasions around the means-goal as being a reasonable course of action. Constituting the issue of cyber-bullying in this manner is a precondition for asserting state regulation and establishing state presence online through a law regarded as being 'proportional and necessary'. This discursive technique of deceit also acts as a deviation from non-criminal justice system interventions or non-governmental initiatives that may be more conducive to address cyber-bullying (see Srivastava, Gamble and Boey 2013). Proponents therefore contend that the most desirable means to deal with cyber-bullying issues are state-driven, criminal justice enforcement-led actions. As MP Wallace (2014) had argued,

> My hope is that as we attack [problems of cyberbullying] through the police, the judicial system, and our criminal court system, and that as those who are committing these crimes are found guilty, it will be a wake-up call to *end* cyberbullying. It is a process that will not happen overnight, but it is one that we need to start (emphasis added, 4625).

Discursive formations such as these also reflect the ways in which ruling groups (i.e. the GoC) attempt to convince non-ruling groups (i.e. the public) to then accept certain policy measures by convincing them that such measure(s) are necessary to protect members of society (especially those who are most vulnerable). For instance, MP Bob Dechert (2014) argued, "What we need to do is to give law enforcement the tools to protect the people who can't protect themselves" (9). Accordingly, lawful access sought to garner support to 'end' cyber-bullying actions (in a narrow respect) while embodying numerous, unrelated elements from previous failed proposals and highly controversial Acts. The Government de jour's pro-punishment stance on this issue is indicative of other punitive trend that call for mandatory minimum sentences, raising the limits for life sentences and removing the ability for certain offenders to apply for parole. In many ways, the Government needs to help keep the 'struggle' of battling cybercrime and cyber-bullying vivid in memory; there are little if any incentives to eradicate its totality, as MP Wallace suggested, as doing so would eliminate law enforcement's need for the powers embodied within lawful access.

Again, an obtained 'backstage' document from the DoJ (request #A-2013-00991) noted: "Bill C-30 proposes to enact a new statute…to amend existing statutes…in order to ensure law enforcement and national security agencies have up-to-date investigative tools, *while ensuring appropriate privacy protections are maintained*" (emphasis added, 46). This argument is reflected around discourses surrounding Bill C-13; that is, with the addition of 7 clauses that directly deal with one aspect of cyberbullying. To this end, the

internal documents by the DoJ surrounding C-13's predecessor appear more forthcoming in its intended purpose. Questions still remain as to whether Bill C-13 will actually bring forward appropriate measures to protect or maintain Canadian privacy at its current level, as policing and surveillance efforts can have the opposite effect[37].

As MP Claude Gravelle (2013:1519) argued, Bill C-13 contains many "things that have nothing to do with cyberbullying. For example, there is a subclause on terrorists and something else on people who steal cable television signals". MP Borg (2014) argued, its ambiguous nature thus "shows a lack of respect [for victims]…we should be debating just cyberbullying. It's too important, and the victims deserve more" (1523). MP Sims (2014) argued that "[this] is another example of legislation where the government has cobbled together various pieces of its agenda and thrown in something on which I would say we have unanimous agreement" (4613). Whereas MP Péclet (2013) had highlighted the fact that it "includes clauses on cyberbullying. However, those clauses cover only offences of a sexual nature. They refer to the non-consensual distribution of intimate images" (1517).

Most parliamentarians and perhaps members of 'civil society' agree: the issue of cyberbullying requires prudent attention and care to assist potential and real victims and to prosecute offenders[38]. Yet when the government de jour uses *one* policy proposal as an 'omnibus' to reign in other frameworks, it is easy for proponents to retort to those that do

---

[37] For instance, Neighborhood Watch programs (see Rosenbaum 1987), stop-and-frisk programs in New York City (see Fagan and Davies 2000), and Canada's inter-agency Combating Violent Extremism Working Group (see Monaghan 2014).

[38] For instance, the NDP introduced Bill C-540 in 2013 to address cyberbullying while containing a section nearly identical to clauses put forward in Bill C-13 around consent and distribution of intimate images. However, when MPs to the NDP brought this fact forward to House of Commons, MP Mike Wallace (2014) argued that without additional elements, which C-13 proposes, the NDP's cyberbullying provisions would have rather only remained "an offence on paper with no real effect" (4618).

not support its tenets as being *against* victims of cyberbullying, or as we have seen with other statements in earlier iterations of lawful access by Vic Toews (2013), being *with* child pornographers. As MP Garrison (2014) argued, "It makes it very difficult for us as members of Parliament to debate and vote on bills when the government has a bunch of unrelated things put into the same bill" (4581)[39]. Further, as MP Rosane Lefebvre (2013) argued, "[the Conservatives] often say that we voted against such and such a measure. However, these are small-scale measures included in gigantic omnibus bills with hundreds of pages. We cannot agree to everything they contain" (1542). This is why, for instance, MP Boivin (2013) sought to split C-13 into two section by seeking "unanimous consent" to then allow the House to expedite cyberbullying portions ("clauses 2 to 7 and 27") while the remaining more 'controversial' elements could receive lengthier debate and care (1442). This proposition ultimately did not succeed in receiving the necessary vote. Still, Amanda Todd's mother, Carol Todd (2014), had made a final plea for the C-13 to be split at Committee where amendments were proposed,

> On my own behalf, I have one request. If there is any way we can separate these controversial provisions from the law designed to help other Canadians avoid the pain experienced by Rehtaeh and my Amanda, I would support that process. This would allow this bill to be free of controversy and to permit a thoughtful and careful review of the privacy-related provisions that have received broad opposition. I do not want my privacy invaded. I don't want young people's privacy compromised. I don't want personal information being exploited, without a protection order that would support individuals. I do not want any Canadian hurt in my daughter's name. I want

---

[39] This routine practice is also why MP Peter Stoffer (2015) recently introduced Bill C-654, which "would stop omnibus legislation from coming in. Legislation could only be introduced if attachments were related to the subject matter". This is principally due to the fact that when large proposals are introduced, "Nobody in the House of Commons properly does the job we need to do to have fiscal scrutiny of the government" therefore arguing the fact that "[he] is [in the House] under false pretenses, and so is every single one of the members of Parliament" (N.P.).

> her legacy to continue to promote hope, celebrate our differences, and give strength to other young people every where (2).

This emotional statement, however, had no effect. Moreover, *no* recommendations or *any* amendments forwarded by any MP, expert, or other public interveners were considered or brought into being. As Gregory Gilhooly (2014) remarked in Committee, Carol Todd's statements were brave as she noted that she did not want her daughter's name to be used as the GoC's scapegoat for bringing in new, invasive laws. However, he also notes that, "at the same time, she advocat[ed] for tougher tools for the police. You can't have it spelled out any more clearly for you than the fact that there is a delicate dynamic: the balance is going to tip one-way or the other eventually" (2). Coming from a deterministic perspective, Gilhooly suggests that privacy and surveillance are antonyms: each is then in conflict and in opposition to the other. Regarding the construction of cyberbullying, MP Sean Casey (2013) argued,

> Bill C-13, we were told, was to address cyberbullying. It would appear, however, that the Conservative government knowingly used this highly emotional issue as a cover to include legislative measures that have nothing to do with cyberbullying. Conflating, for example, terrorism with cyberbullying does not make any sense. Furthermore, using the scourge of cyberbullying in order to resurrect elements of the infamous Bill C-30, a piece of legislative work wholly rejected because it was in effect an e-snooping bill, is wrong…[the] government seems to be using victims of cyberbullying for political and partisan reasons (1445).

Framing C-13 as a 'combating-cyberbullying-bill' reflects the fact that there are clear and fundamental expectations in democracy; citizens expect certain legal rights, liberties and personal freedoms. Ruling elites should not therefore dominate with 'iron-fists' (passing laws as they please); so-called democracies must rule by way of ideas even if these ideas

are not an authentic exposé (Gramsci 1971; Alexander 2004)[40]. To therefore preserve the status quo, "sovereign power has to govern through rights and freedoms, not coercion and force" (Vrasti 2012:124). To subjugate populations, elites manufacture consent through discursive enactments by drawing upon specific moral panic(s) (e.g. an online predator, cyberbully or terrorist). This process can transpire through hyperbolic reactions delivered through the mass media, state representatives and the criminal justice system. C-13 thus attempts to legitimize state activities and new powers by convincing the public that an absence of a response to a particular problem may somehow cause even greater harm.

Drawing upon emotional appeal, Peter MacKay (2014) argued, "had this law been in place [victims of cyberbullying in Canada] would still be with us today" (5595). This dialectical relationship between the 'official' discourse and a more highly sensitive public element reflects the significance of presenting state policies in a format, framing "desires as facts" in order to garner public support around the C-13's hypothesized capacities, and "imaginaries of interested policies as the way the world actually is" or could have been had such measures been in place (see Fairclough 2001:240). As David Fraser noted in the Committee debates, "It has been suggested that Bill C-13, if it had been enforced, could have saved Amanda Todd and Rehtaeh Parsons and other young people. That makes a good sound bite, but the world is much more complicated than that" (1). Fraser's notion

---

[40] The critical issue in this regard is that ruling elites (especially those in Government) should not be able to fraudulently and deliberately fabricate "Truths" on the public stage and yet hide behind *Access to Information* and *Freedom of Information* laws where the alternative narratives live. Disrupting official narratives through ATI can erode public trust and undermine authoritative institutions leading perhaps to chaos. We cannot live without Government and Law, but that does not mean an erosion of public trust will not allow us to revisit the issues and learn from them (albeit painfully if need be).

was iterated by Jaffer (2014:13) in Senate debates arguing, “Amanda Todd’s and Rehtaeh Parsons’ lives would have been no different if this bill had been enacted earlier”.

In many ways, the proponents loosely act as propagandist agents, which Leonard Doob (1948) defines as **“**the attempt to affect the personalities and to control the behavior of individuals toward ends considered unscientific or of doubtful value in a society at a particular time” (390). This is a move alongside 'persuasive elements involving “debate, discussion, and careful consideration of options” (Pratkanis and Turner 1996:191), which we can certainly say existed in Committee deliberations. As Lippman (1921) has argued, actors positioned as leaders in any organization (e.g. the Government) are to some degree ‘propagandists’ to the extent that they can “decide more and more consciously what facts, in what setting, in what guise [they] shall permit the public to know” (162) about some artifact, policy, institution, law or whatever else. To this degree we can understand that all relationships are perhaps “characterized by the ratio of secrecy that is involved in it”, as Simmel (1906:462) once noted, in terms of the rhetoric and rationale surrounding the framing of lawful access discourse to manufacture consent between the Government and public generally[41]. Indeed, as Lippman (1921) has noted, “the manufacture of consent…is not a new art...it has, in fact, improved enormously in ethic, because it is now based on analysis rather than on the rule of thumb” (162). Critical to this process is that the *Access to Information Act* may sometimes allow us to understand and to capture instances where the Government promotes one thing publicly but yet embody alterity displays on a ‘front

---

[41] As one ‘unofficial’ Public Safety record (request #A-2012-01994) authored by their National Security Group notes, “government must maintain some degree of security and confidentiality in order to function” (citing *R. v. Thomson* [1992] 1 S.C.R. 385). The goal is to “balanc[e] the competing public interests in disclosure and non-disclosure and have extended the range of options regarding the disposition of information” (91-92).

stage'. While some may expect workers or representatives of the state to promote policies that may be unfavorable to particular segments of society, we do not necessarily expect to see the same actors be unconvinced of their own position privately yet keep promoting it publicly, of which can be revealed through access to information records. One query and concern in this regard is that the deliberate fabrication of 'Truth' through discourse, doing so by cunning manufacturing, can cause ripples in the fabric of trust that states try to sew.

In the case where the Conservatives held a majority government, it can be argued that careful and prudent analysis was, in reality, neither necessary nor did consent need to be manufactured at all. Lawful access would have been enacted regardless, as the Party held enough seats in the House of Commons to pass its tenets to the Senate for review, which is dominated by sitting senators appointed by the Governor General and under the counsel of the Prime Minister him or herself. This is of course to say that the Senate is unelected and therefore may serve agendas of the Government de jour despite being the chamber of 'sober' second thought[42]. As Lamontagne (1969) notes, policy-making within Parliament is traditionally concerned with the notion that "in the House of Commons, the opposition could speak as long as it wished but it would have been a great sign of weakness on the part of a minister to accept any of [their] suggestions" (133). To such an end, the Conservatives held themselves to more traditional roles around policy-making in regards to lawful access and other recently introduced Bills (e.g. Bill C-51 or the 'Anti-

[42] This issue has cased concern in Canada in recent years. For instance, the New Democratic Party called for the Senate to be reformed or abolished altogether with their "Roll Up the Red Carpet" (2014) campaign, which argued, "Unelected, unaccountable senators represent the parties that appoint them – not the Canadian people" (N.P.).

Terrorism Act'). This is perhaps why little consideration was given to every amendment proposed by Parliamentarians at the Committee stage; none of which were adopted.

To this end, we may agree with the concepts put forward by Goffman (1959) that performances are *given* to the public using the 'front stage' (e.g. House of Commons) of government displays based on expressions *given off*. The 'front stage' is a place offering us the sense that there was potential for lawful access to be 'fairly' debated and amended accordingly through counter-discourse. However, it is difficult to discern this possibility ever existed, as a majority rule in Parliament allows government to do away with nearly any law they introduce (although certain checks and balances are said to stand to prevent unbalanced rule or unconstitutional policies).

As John Stuart Mill (1989) has argued, "Like other tyrannies, the tyranny of the majority was at first, and is still vulgarly, held in dread, chiefly as operating through the acts of the public authorities" (8). Again, being a matter of Liberty and Authority (5) or of Privacy and Surveillance, which Gilhooly (2014:2) remarked in Committee debates, "the balance is going to tip one way or the other eventually". We are left therefore with an understanding that democratic processes are alive, remarkable and convincingly real (Alexander 2004) through 'authentic' exposés in the legislature and at other stages (32). However, when we step back to consider that the present Government held a majority and lawful access would have proceeded regardless of debate or even *all* opposition by Members of Parliament and other interveners, we are left asking larger questions around the 'fairness' in the rule of governance[43]. This is important to consider as certain checks

[43] This is not to say that *only* the Conservatives would have proceeded in this manner; the Liberal Party or New Democratic Party could have equally done the same.

and balances (e.g. the Supreme Court) have often made declarations against the policies of Conservatives. Still, the Conservatives steadily challenge the Supreme Court authority when their rulings become antithetical to the regime's carefully fabricated agendas[44].

The next section questions the validity of the former Minister's (2013) argument that C-13 is about putting "police investigative powers in place on the Internet" through "legislation that would enable police to do their job properly" (1440). Given the former Minister's presupposition that present frameworks do not allow policing and intelligence agencies to "do their job properly", the validity of this argument is interrogated via 'front stage' discourse and 'backstage' texts obtained through the *Access to Information Act*.

5.3 An Absence of Investigative Policing Powers?

Proponents of lawful access legislation have repeatedly argued in Canada's House of Commons that, "As politicians we have seen the dark side of the Internet…times have changed incredibly, and we need to change with the times…the need for these tools is obvious" (McLeod 2014:4582). As Internet usage has increased globally, Canadian law enforcement agencies have been adamant to state the significance of improving electronic surveillance structures to detect and to preempt regular criminal acts and/or oddities like (cyber) terrorism by accessing subscriber metadata and other digital information. This is principally due to the fact that the Internet has now provided an additional platform for committing new crimes, such as computer hacking, as well as "old crimes in new ways", such as fraud (RCMP 2014:14). Accordingly, the prevailing notion among the police has been that increased access to user metadata will therefore result in increased security and

[44] E.g. physician-assisted suicide debates (see *Carter v Carter 2015*) or stance against the release of Omar Khadr, a Canadian citizen tortured by American military forces.

a reduction in overall harm, which therefore improves public safety and security online and offline. As one internal document from the DoJ (request #A-2013-00991) has stated, "Technology has evolved considerably…and Canada's laws have not kept pace" (23).

Canadian policing agencies have had a number of legal tools to lawfully access user metadata and digital information for some time. Moreover, lawful access law C-13 has created additional means. First, police can use judicially authorized warrants, which allow for a search of criminal evidence as policing agencies may seize any computer data, transmission data and/or tracking data. Warrants presuppose that person(s) of interest has committed a *Criminal Code* offence or that there are reasonable grounds to believe that an offence will be committed. This involves court oversight and its consequences are a part of the public record therefore presenting a degree of transparency within the legal process.

Secondly, C-13 created what are called "production orders". Nicol and Valiquet (2014) argue, this requires a "person in possession of the information [in question to] produce it on request, whereas under a search warrant, the law enforcement agency goes to the site to obtain the information by searching for it and seizing it" (12). With Bill C-13, this allows for the capture of 'transmission data' (i.e. metadata under section 487.016) and 'tracking data' (i.e. locations of objects such as a computer and therefore the person possessing the technology under section 487.017 of the *Criminal Code*).

Thirdly, there are now "preservation demands". Former Minister MacKay (2014) argued that these are essentially "do not delete" orders made out to those in possession of computer data to therefore help preserve evidence destruction (2); that is, it's "about the preservation of a virtual crime scene" (7). In this case, law enforcement agencies can ask a TSP/ISP or anyone in possession of any digital information to preserve it for a specified

period of time or until a warrant allows for the lawful seizure of the data in question. In a sense, preservation demands freeze the data, acting as a type of "pre-warrant" as Public Safety (request #A-2012-00113:102) records have shown in order to *guarantee* data will remain available for procurement at a later date. Nicol and Valiquet (2014:11) argue, in addition to the means above, TSPs/ISPs may also voluntarily provide user metadata to law enforcement and national security agencies absent of the three above methods and devoid of any legal reprisal under the newly created Section 487.0195 of the *Criminal Code*.

Accordingly, metadata can be obtained in this fourth manner by way of voluntary disclosures of information by third parties. Since the very inception of Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) over a decade ago, this practice has been authorized congruent to Section 7(3)(c.1)[45] and in accordance with the *Privacy Act*. Canada's *Criminal Code* also facilitates voluntary disclosures. In fact, it goes further than PIPEDA, as it grants immunity for criminal or civil proceedings to those who make a disclosure under declarations of "good faith" and "reasonableness" (Section 25).

In the famous case of *R. v. Duarte* [1990:45], the Supreme Court justice La Forest dissented, "Law enforcement must always seek prior *judicial authorization* before using electronic surveillance". As Jason Young (2004) has argued,

---

[45] PIPEDA states, "Disclosure without knowledge of consent…made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs, (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or (iii) the disclosure is requested for the purpose of administering any law of Canada or a province" (Section 7(3)(c.1)).

> The rationale for this framework is so obvious that in democratic societies it is sometimes taken for granted…the very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to *annihilate* any expectation that our communications will remain private. Ergo, it is unacceptable in a free society that law enforcement be allowed to invade citizens' privacy at their sole discretion or that they be allowed to circumscribe rights through technology that they could not in law (9).

In Canada, however, obtaining user metadata is *not* considered to be a form of electronic surveillance, as it does not include the *content* of communications whereas reasonable expectations of privacy do in fact apply. That is to say, procuring and sifting through user metadata is regarded as a form of 'non-surveillance'. It is something perceived by the GoC and law enforcement as a different kind. This phenomenon is not unique to Canadian Internet governance and policing-surveillance activities done digitally. For instance, in the United States—as Senator Dianne Feinstein (2013:N.P.) once argued in response to the massive surveillance programs disclosed by extensive leaks from Edward Snowden—the American practices are regarded to not constitute any form of "surveillance" as programs "do not collect the content of any communication". Nonetheless, Senator Feinstein fails to acknowledge that metadata collection without question or rigorous oversight can result in the collection of communications content.

As Young (2004) notes, the *Criminal Code* "generally provide[s] that state agencies cannot obtain documents or information without first establishing a factual foundation of 'reasonable and probable' grounds that an offence has been or will be committed" (2). However, as we shall see, this has not been the practice for Canadian law enforcement agents although it remains a *theoretical* tenet of Law; raising questions around whether metadata is less sensitive than communications content, which chapter three explored, and

if metadata may be regarded as a type of 'non-information'. That is, being of a different kind entirely, as such information capturing is considered as an act of 'non-surveillance'.

Canada's former Privacy Commissioner, Jennifer Stoddart (2007), has argued in her consultation paper on metadata that there is a prevailing notion among law enforcement agencies that metadata "information carries a low expectation of privacy and as such does not require judicial authorization" to be lawfully obtained (6). Still, "CNA information[46] may be valuable to LE/NS[47] agencies specifically because it can provide access to even more sensitive information" (ibid) than communications content. Stoddart concluded that given this, protection for Canadian user telephony metadata information should exist,

> Neither this consultation paper nor previous consultation documents has presented a compelling case based, on empirical evidence, that the inability to obtain CNA in a timely way has created serious problems for LE/NS agencies in Canada. This calls into question the policy rationale from both a proportionality and necessity perspective. Second, it is our view that a reasonable expectation of privacy attaches to CNA data. This renders any mandatory disclosure/seizure regime of dubious constitutional validity (8)[48].

Since the publication of Stoddart's consultation paper, policing agencies have searched for almost any empirical evidence to support the arguments for obtaining metadata absent

---

[46] "CNA" means *Customer Name and Address Information*, which is analogous to Basic Subscriber Indentifying (BSI) Information (i.e. metadata) (Privacy Commissioner Canada 2007). The Privacy Commissioner (2013) notes, this includes: name, address, telephone number, e-mail address, IP address, and local service provider identifier (1). Documents by Public Safety Canada (request #A-2012-00113) further confirm this definition (103).

[47] Law Enforcement (LE) and National Security (LS).

[48] Interestingly, an email by a Public Safety (request #A-2013-00261) worker notes, "IP addresses, email addresses, and other electronic identifiers are key pieces of evidence in investigations of cyber-crime. It is *rare* that a suspect name is provided at the beginning of an investigation" (emphasis added, 492). Meanwhile, a report by the Ombudsman for Victims of Crime (2007) notes, "Obtaining a suspect's name and address is already common practice during an investigation"; analogizing such a requests to a police stop where a driver provide their driver's licence. The difference, however, is that in the latter example, a driver can 'see' that they are subject to surveillance whereas notification for digital surveillance is not compulsory and would only be revealed if a case goes to court.

of a warrant[49]. Still, Bill C-13 further codifies the tools for obtaining metadata and other information. Under section 487.0195(1) and subsection 2, it now states that those "who preserves data or provides a document" to a "peace officer or public officer" will *not* "incur any criminal or civil liability for doing so" if disclosures are not prohibited by Law. According to Michael Geist, this tenet is highly problematic. In the Committee debates, Geist (2014a) argued that immunity would be granted in cases "even when disclosures are unreasonable" (5), as it does not require disclosures to be made under principles of 'good faith', as articulated under Section 25 of the *Code*. The inclusion of "public officers" also means metadata can be obtained by public servants ranging "from tax agents to sheriffs, reeves, justice of the peace, CSIS agents, and even, yes, mayors" (Ling 2014, N.P.)[50].

Cara Zwibel (2014), lawyer and program director for the Canadian Civil Liberties Association (CCLA), expressed the CCLA's concerns on this new Section in Committee debates, arguing, "The immunity provision is in our view a blatant attempt to incentivize private corporations to cooperate with law enforcement, even when doing so poses a genuine risk to customer privacy and may not serve any compelling state objective" (5). MP Sean Casey (2014) also expressed his concerns with lucidity, noting that the current system prevents the ability to know whether one's personal data has ever been disclosed to a third-party when facilitated under PIPEDA (10).

---

[49] This can be observed in internal emails and discussions in the following ATI requests: Public Safety (requests #A-2012-00113 and A-2013-00261), Security Intelligence Review Committee (request #A-2010-07), and RCMP (A-2011-06549).

[50] In Australia, recent statistics indicate that local councilors are using powers provided by similar lawful access legislation to collect metadata on residents without a warrant in order to go after bylaw infractions such as unregistered pets (Francis 2015). Questions are raised whether comparable practices will be observed in Canada.

David Fraser (2014), an Internet and privacy lawyer, stated in the Committee, that if a third-party provides data to law enforcement or anyone under paragraph 7(3)(c.1) of PIPEDA, and a Canadian "customer then says 'Did you hand over my information?' the [third-party]…has to go to the [requester] and ask them for permission to hand over [that] information…the legislation imposes a gag order" (10). This practice is in stark contrast to similar data procuring activities of the state, such as wiretap authorizations, whereby a person who is a subject to a wiretap must be notified that such activity took place within a 60-day period following an investigation[51]. David Spratt (2014) expressed his concern over the lack of notification requirements in Committee regarding Section 487.0195 of C-13 and paragraph 7(3)(c.1) of PIPEDA. Interestingly, on this topic, MP Wilks (2014), argued, "To say that people are not notified is utterly wrong; they are notified within 60 days" (16). To which Spratt replied, "Show me the notification in the bill. It's not there" (ibid). With certitude, Wilks assured, "It is there…I'll show it to you afterward" (ibid). Yet, in exploring the contents of Bill C-13, there are indeed no notification requirements. Moreover, as David Spratt (2014) pointed out in Committee, "The minister said that the obligation to disclose to an individual when their information has been disclosed was covered under PIPEDA. It's not" (10). This reflects the extent that even proponents who supported lawful access did not fully understand its varying consequences and potential impacts on Canadians. MP Peter Stoffer's (2015) comments exemplify this issue with clarity: "When legislation comes forward with 418 pages that would change 50 statutes and laws, nobody in the House of Commons reads it. Nobody in the House of Commons

---

[51] The Conservatives recently introduced amendments to this notification period under the *Anti-Terrorism Act* (C-51) where the standard has gone from 60 days to one year.

properly does the job we need to do to have fiscal scrutiny of the government" (11385). Stoffer therefore proposed C-654 to "stop omnibus legislation from coming in" (ibid)[52].

Interestingly, on the topic of disclosures, the Conservative government's tone on the matter dramatically changed at later stages of debates. In the final Committee meeting where MPs had opportunity to propose amendments to lawful access, MP Péclet (2014:5) forwarded paragraph 487.0191(1)(a), which argued, "People whose personal information has been shared with other organizations during an investigation or electronic surveillance" be notified in writing that this took place. This proposition was influenced by witnesses in Committee debates, which raised concerns around the "new powers" for police absent of "oversight and information mechanisms" (4). Yet this time, MP Dechert did not support her proposal under the idea that, "Notification jeopardizes investigations and often results in the deletion and destruction of evidence" (5). However, this argument does not stand on its own merit; notifications only occur *after* investigations conclude.

In a study conducted by the University of Toronto's Citizen Lab's Chris Parsons (2014), it is also unclear whether any Canadian ISP/TSP currently notify customers when disclosure requests are made and submitted to law enforcement agencies or to any other third party for that matter. It is also worth noting, that MP Dechert—Parliament Secretary to the Minister of Justice—neither supported Péclet's amendment nor *any* other proposal made by any MP, expert witness, member of the public or anyone else. Accordingly, Bill

---

[52] Interestingly, when debating lawful access law, Stoffer (2013) remarked: "I know it is rather unusual for me to ask a question when it comes to anything regarding the Internet and computers because I do not use them" (1541) and "It is rather ironic that I am talking about cyberbullying when I myself do not even use a computer, smart phone or BlackBerry in any way, shape or form" (1569). Accordingly, it is worrisome that many within parliament vote and shape real policies that have real impacts on the lived realities of Canadians without an appreciable understanding of the potential affects of the Acts.

C-13 has remained unchanged from its initial proposal despite moving through multiple legislative stages, including both the House of Commons and Senate Committee debates. Suffice it to say, it was held that Bill C-13 was unblemished, which is a common trend observed with other bills introduced by the Conservatives in recent years. As MP Wayne Easter (2014) has argued on this particular issue, "the way the Conservative government operates in committee has undermined the committee process, and it is undermining the very essence of how democracy works in this country" (8119).

Fraser (2014) summarized the gravity of Bill C-13's immunity provision well. Consider his analogy: "I may not be legally prohibited from accidently driving my car into yours, but if I do that, you're entitled to damages from that. I should be paying for the harm that is caused" (3). Bill C-13's S. 487.0195(1) and subsection (2) effectively eliminates this right of claim and disclosures no longer need to meet the good faith or reasonableness thresholds. Fraser agued, "[this] will only encourage overreaching by law enforcement" (3). To the extent that individual privacy, for instance, is infringed due to disclosures of metadata information, users are then unaware this process took place and therefore are unable to seek any remediation for a potential *Charter* infringement whereas the *Charter* provides that one "may apply to a court of competent jurisdiction to obtain such remedy" under Section 24. Given that user metadata is procured absent of judicial authorization and therefore any court oversight, police and national agencies also do not need to meet the Oakes (1986) test, which has historically been used by a court judge to determine if state actions demonstrably justify a violation of *Charter* rights[53].

---

[53] C-51 compounds this issue by allowing national security agents to violate *Charter* rights under secret approvals to a court. Given that judges are *appointed* in Canada, there

The absence of notification requirements for disclosures of personal metadata information has serious implications on privacy. It reflects the fact that electronic and Big Data surveillance practices often exist outside of user awareness (Van Dijck 2014:200). Couple this with built-in mechanisms preventing users from knowing whether personal data has ever been disclosed to third parties, reduces transparency of networked policing practices and also raises fundamental epistemological and ontological questions around personal autonomy and existing degrees of secrecy within 'policing' agency structures. Moreover, it raises concerns around the future state of *Charter* rights and their treatment by law enforcement agencies, as Government policies activate and introduce measures that permit such violation. This is most certainly perplexing, for instance, as an access to information record reveals that law enforcement agencies have actually carried out mass 'surveillance' in cases where "no criminal offence is under investigation" (Public Safety request #A-2012-00113:39) via voluntary disclosures, of which the following subsection will explore. Non-criminal investigation as a result of TSP user metadata disclosures in particular raises questions around paragraph 7(3)(c.1) of PIPEDA and the constitutional validity of these longstanding practices of Canadian policing and surveillance agencies.

---

is ample reason to speculate that ideologically leaning judges may be inclined to facilitate such requests. A PowerPoint document by the DoJ (request #A-2013-00991) entitled "Streamlined process for related warrants and new safeguard" states a need to "Provide a single process for obtaining court orders relating to an investigation for which an interception authorization was obtained". This "reduces delay by going to one judge instead of several, introduces a consistent authorization timeframe for all investigative techniques, increases safety by *automatically sealing all warrants* related to the interception investigation from disclosure"(emphasis added, 65). As this document illustrates, there is perhaps other impending changes and updates to the criminal justice system to come, of which will be the creation of a streamlined warrant approval process while doing so entirely under seal (i.e. in secret) by default; that is, secrecy by design. Such design may be analogous to the Foreign Intelligence Surveillance (FISA) courts in the United States, which have recently come under fire since the Snowden revelations.

To this end, MP Turk (2014) has argued, “Civil or criminal liability exemption for ISPs invites ISPs to aid invasive state surveillance rather than incentivizing ISPs to protect Canadians' personal information with political and legal means” (10). Lawful access provisions therefore “essentially offers an incentive for the ISPs to think of their relationship with the government, not of their obligations to their subscribers” (13). Canadian Privacy Commissioner, Daniel Therrien (2014), argued that this new section is “send[ing] a strong signal to telecommunications companies, to enhance the voluntary disclosure that is currently occurring” (5). Meanwhile, despite this powerful provision that limits the liability for TSPs and ISPs, no witness from any TSP or ISP who may ultimately benefit from these legal amendments appeared before committee or any other legislative stage, as Dusseault (2014) has noted[54]. The next section interrogates Therrien’s question around the scope of voluntary disclosures and the issue of ‘non-surveillance’.

5.3.1 The Scope of Electronic ‘Non-Surveillance’ in Canada

The scope of state and corporate surveillance frequently captures the attention and stirs the imaginations of citizens across time and space. The events of 9/11 were followed by new shifts in policing and surveillance policies. Following the attacks in the United States, many governments reigned in variegated invasive measures to detect prospective adversarial attacks while equally trying to comprehend some of the circumstances that led to this tragic event. Equally, socio-economic dependency and reliance toward the ‘boom’

[54] He stated in Committee debates, “I am rather surprised to hear that no witnesses from telephone companies, telecommunications companies or Internet service providers appeared before the committee. I am rather surprised that these types of companies were not called upon to testify given that they share vast amounts of information” (7670).

of technology within the West was paralleled by a rise toward greater domestic usage of the World Wide Web (WWW). Accordingly, it is no surprise then that these spheres have intersected to represent surveillance through and toward technologies of every day life.

Recently, many have learned about the widespread, dragnet surveillance practices existing within the United States as well as among other government allies part of the *Five Eyes*, including Canada. We learned that the US Government conducts routine, mass surveillance against its own population and foreign nation states by actively recording every thing from phone calls and text messages to taking measures to weaken the actual technological infrastructure of the likes of Yahoo! and Google to gain access to basic subscriber information and basic user metadata (Greenwald 2014). In Canada, electronic surveillance practices of law enforcement and of other national security agencies have remained relatively unknown to its own population and global world. Canada is a much smaller player on the 'international stage' and commands much less attention politically, militarily and economically in comparison to the United States. This in certain ways has afforded Canadian structures to 'function' with a higher degree of secrecy in their every day practices, as the world appears less concerned with the activities of smaller, northern neighbors. Still, routine and extensive use of Canada's *Access to Information Act* and international leaks has provided evidence of the scope of 'non-surveillance' and regular, normalized and routine procurement of metadata information among a mosaic of policing agencies over the past decade.

In one internal document by Public Safety (request #A-2012-00113), an email communication reveals that the Integrated Threat Assessment Centre (ITAC)—a federal agency that collects and analyzes intelligence from GoC agencies—"handled 1,130,000

BSI requests annually from 2006-2008[55]" (122). Moreover, "In other areas, police obtain [user metadata information] voluntarily due to a cooperative relationship with the TSP". Yet the request "doesn't get recorded" and "negative response[s]…doesn't get recorded". Meanwhile, "refusals from TSPs–that doesn't get recorded" either (ibid). Interestingly, in discussion around Bill C-30, this Bill would have "mandate[d] authorities to determine – and audit–exactly what is being requested, what is being provided, and why" (ibid). And still, such reporting proposals were not carried forward with respect to the next iteration, C-13. When it comes to accessing metadata, documents show that police often use a tool called "Form 6306", which was "developed to try to obtain numbers on subscriber info requests" by the RCMP (110). Interestingly, this document notes that when it comes to a metadata request to an ISP/TSP there is a "93% *success rate*" in compliance (emphasis added, 111). Despite such high compliance rates, the RCMP argue, "One of the problems with current system is that there is no uniformity or reliability as to how/if TSPs respond to requests for basic subscriber information" (77).

In addition to this vast amount of disclosures taking place, we can also say that there are severe data documentation flaws for the RCMP and ITAC. Records reveal there is little, if any, external pressure to compel either to address documentation issues at this front, as a number of disclosures are not recorded. This of course is not an issue unique to this specific activity by the police or of other governmental reporting generally. However, this issue has persisted for many years. As Young (2004) notes in his examination of the

---

[55] Basic Subscriber Information is known also as Customer Name and Address (CNA) information. BSI and CNA information are both conceptualized here under one rubric: metadata. According to Canada's Privacy Commissioner (2013), BSI is synonymous with CNA and can include: name, address, telephone number, electronic mail address, Internet protocol address, and local service provider identifier (1).

Solicitor-General's *Annual Report on the Use of Electronic Surveillance* (2003), the "Solicitor-General does not even collect statistics on the frequency for which intercepts are authorized" (4). To this extent, it is difficult to instill public confidence in the record keeping abilities of law enforcement regarding these practices that collect large troves of user metadata on the private lives of Canadians (especially those who are not subject to a criminal investigation). As one consequence, external bodies are hindered from auditing state and corporate activities, which has implications for Canadian privacy. Perhaps most troublesome in this regard, as Therrien (2014:4) noted in a Committee debates on C-13, "There are no requirements in the bill to report on the extent of the use of any of the new powers…this is of serious concern, especially given the range of officers who can exercise these powers and the possible effects of extending legal immunity". Ultimately, these figures reflect the incompleteness and do not accurately capture breadth or scope of 'Big Data' surveillance since there are no existing or robust systems that count the actual number of disclosures, which much like inaccuracies found within crime rate statistics[56] (popularly known as the 'dark figure' of crime), there is a reduction then in "the accuracy of inferences from the data" that may therefore be derived (Skogan 1977:42).

As Skogan has noted in relation to crime, this *dark figure* is known to be the many activities that go unreported and unrecorded. In a similar way, comparison can be made to the recording or rather lack of documentation for user metadata requests. If we accept this argument, we can therefore infer that there were more than 1,130,000 requests annually between 2006 and 2008, as voluntary disclosures are not recorded in any systematic way.

---

[56] As Greg Jenion's (2010) work iterates, "police practices can have dramatic effects on criminal incident reports and ultimately the reporting of crime rates" (190). In other words, when reporting is low the crime rate will appear low and visa versa.

An access to information record obtained by Michael Geist (2015) compounds this issue: "CNA requests by Canadian law enforcement agencies is not complete as the RCMP reporting tool was not consistently used by RCMP units and other [law enforcement agencies]" (N.P.). Accordingly, data in these records do not reveal quantity of disclosures made by each state department. Still, it is an issue that has existed for years and it appears as though there is no incentive to improve the disclosure reporting. This is concerning, as Public Safety (request #A-2012-00113) records have documented the fact that,

> Obtaining a warrant for general policing duties is not possible because *no criminal offence is under investigation* hence obtaining a warrant is not an option…For either purpose, investigative or to perform general policing duties, it is the position of the police that obtaining a warrant for basic customer identifying information such as CNA is not required by the law" (emphasis added, 39).

To this end, the voluntary disclosure practices is imperative to facilitating this activity of 'non-surveillance', as the police recognize these practices may not actually constitute any lawful access 'search' and therefore depend on TSP/ISP corporate compliance. Moreover, it highlights a critical point, which is that law enforcement is conducting "general policing duties" on the Internet. This is to say, these officers are *walking* a virtual beat, *observing* surroundings and *proactively* engaged in routine practices that are analogous to what we 'see' offline. Yet, we do not 'see' online activities take place and the RCMP has not (to date) communicated this practice to Canadians in an open or transparent manner.

As Geist (2013:N.P.) found in his use of Canada's *Access to Information Act*, the Canadian Border Service Agency (CBSA) made "18,849 requests in [2012] for subscriber information including geolocation and call records. The CBSA obtained a warrant in 52 cases with all other cases involving a simple request without court oversight". Further, an entire for-profit industry has arisen around voluntary metadata disclosures. He discovered,

"The telecom providers fulfilled the requests virtually every time–18,824–and the CBSA paid $1.00 and $3.00 per request" (ibid)[57]. Compliance governed through such economic incentives reflect the notion that 'crime control alliances' (Garland 1996:455) often enroll actors in the production of security through mechanisms that benefit each party among a coordinated network. Law enforcement agencies benefit from access afforded through the partnership. Meanwhile, TSPs/ISPs are compensated for services, all of which is done of course at the expense of the privacy of paying Canadian subscribers.

In addition to what I refer to the above as a *pay-per-view-disclosure* system, Geist (2014) reveals that there is also a "Bell Canada Law Enforcement database", which allows GoC departments to access data readily available in their servers. This raises significant questions around whether TSPs/ISPs are proactively developing systems permitting state agencies to have unfettered access to subscriber data at a cost. Details of what information is included or excluded from disclosures remains unclear. The database is in many ways analogous to *ICREACH*, which as leaks from Snowden reveal, is a "'Google-like' search engine built to share more than 850 billion records about phone calls, emails, cell phone locations, and Internet chats" to the *Five Eyes'* stakeholders (Gallagher 2014). In the case of the CBSA disclosures, MP Borg (2014) argued in House of Commons debates,

> Only 2 of [the 18,849] requests were listed as being required for national security reasons…*there is no transparency. There is absolutely no oversight.* When I asked the government in writing for the data for the past 10 years from all agencies, it did not have the data [on the quantity of disclosures and/or quantity by department] (emphasis added, 8121-8122).

---

[57] TSPs have also engaged in other for-profit endeavors. For instance, Bell Canada was recently subject to a $750-million class-action lawsuit for a "controversial Relevant Ads Program that allegedly tracked, collected and sold its customers' and Virgin Mobile users' Internet browsing data" to third parties (Postmedia Network 2015:N.P.)

'Backstage' Public Safety (request #A-2012-00113) records further note, the "[Ontario Provincial Police]…on their own make 10,000 such requests to telco/ISP's"; and stating, "*You can imagine the workload of police services if a warrant is required for such information*" (emphasis added, 60).

Based on the amalgamation of information above, we can say that the RCMP has admitted to conducting 'surveillance' on citizens for non-criminal purposes. This practice is done absent of formal investigation on any basis of probable grounds *to believe* or *to suspect* that a criminal offence has taken place, as required for 'actual', legal surveillance activities. Absent of judicial authorizations and oversight, no legal thresholds thus exist to protect basic notions of privacy for the procurement of metadata and users are unaware of being subject to law enforcement's gaze, as notifications are not compulsory. Moreover, a *pay-per-view-disclosure* system readily exists in Canada. Given also that a large majority of disclosures are made voluntary via paragraph 7(3)(c.1) of *PIPEDA*, which requires that disclosures are made to enforce "law…carrying out an investigation…[or] administering any law", it is unclear if these practices are lawful, as 'backstage' Public Safety (request #A-2012-00113) records have declared, "No criminal offence is under investigation" (39). This raises two critical questions: 1) if there is complete absence of a formal investigation, the absence of enforcement and an absence of administering any law while the disclosure is facilitated through PIPEDA, is this a lawful application of this *Act*? and 2) if not, do any acts of remediation exist for the privacy violations of paying Canadian subscribers?

It is clear that there are not only issues around the data documentation practices of law enforcement, but there are issues in regards to the transparency, oversight and review of these procedures. Likewise, the frequency of requests that pertain to a formal criminal

investigation or also non-criminal cases, as Public Safety documents show, is unclear and perhaps unknowable given the lack of data documentation practices[58]. It is also unsettling and unbeknownst if police want total, unfettered access to metadata to reduce the amount of paperwork in facilitating their duties as public servants, as described above.

To the extent that public agencies 'govern' *through* private intermediaries and due to these data documentation flaws, a system(s) of opacity envelops governance practices, reducing accountability and transparency; that is, precluding anyone to examine potential tenebrous activity. Throughout Canada's history, there are a myriad of examples[59] of the varying consequences, which can emerge when clear checks and balances do not exist in government. Problems of opacity however exist well beyond the contemporary structures of Big Data network surveillance. As one memorandum of understanding by the Director of CSIS (request #A-2013-168) to the Minister of Public Safety in 2012 notes, "The work undertaken by the Service is often highly sensitive and its outcomes little known, limited as they are by the need-to-know principle even within the Government of Canada" (76).

To preserve the integrity and security of the GoC's departments and institutions, secrecy should exist around very specific activities. Indeed, structures of state secrecy are articulated in many Acts (e.g. Access to Information Act and Privacy Act). The purpose

---

[58] A request was submitted to Public Safety Canada and RCMP for "All information (documents, emails) regarding the number of requests to telecommunication service providers and/or Internet service providers for basic subscriber information for criminal and non-criminal investigations between 2006 and 2014". At the time of this research, neither department has completed this formal request.

[59] For example, asset misuse and ethics breaches by CSEC (see Bronskill 2014) and the recently assented 'Anti-Terror Act' (Bill C-51), allowing CSIS agents to violate *Charter Rights* of Canadians under Section 12(3) to 'reduce threats to the security of Canada' via a warrant application to a court, which is done both *ex parte* (i.e. without the person(s) subject to the warrant being present) and in camera (i.e. in secret) (see Forcese 2015).

of these legal articulations is to clearly prevent public disclosures of information or data considered otherwise to be injurious to the Government of Canada if made available[60]. Exemptions include but are certainly not limited to: Cabinet confidences, military tactics or strategies and architectural plans of public government institutions. Yet on the other hand, it is critical that GoC activities not subject to any public scrutiny should embody systems of oversight to ensure democratic processes are upheld to high regards. This is especially true if governments introduce 'new' legal measures, which inflate the powers of police. Failure to do otherwise could tear at the very fabric of democratic societies and contribute to a civil divide between citizens and government by eroding public trust when indecent non-oversight activities become known. Further, if oversight systems exist, the citizens should not depend on singular 'external' bodies made up of citizens or 'experts' appointed by the Government de jour. It would be wise to implement more non-partisan, decentralized structures to ensure that legal, social and ethical practices are maintained to the highest regard in day-to-day format rather than contemporary models, which employ annual review by observers handpicked by the regime in power; such is the case with the CSIS' reactive Security Intelligence Review Committee (SIRC).

As one 'backstage' document from CSIS (request #A-2012-248) notes, "Erosion of authority and heightened distrust in institutions has led to groups like WikiLeaks and individuals like Bradley Manning who have leaked secrets in what they perceive to be in the national interest" (38). Similarly, "With new actors emerging with interests of their own, they will not hesitate to protect and advance these interests. And, of course, who

---

[60] An internal, 'backstage' Public Safety (request #A-2012-01994:97) record defines "potentially injurious information" as "information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security".

can blame them? The West protects and advances its interests as well" (36). Openness and transparency are two mores woven into the fabrics of democratic societies and each are reflected in the provisions contained in Canada's *Constitution* and the *Charter*. To the extent that the GoC drifts away from these basic ideals, support and trust will be lost. If the GoC is indeed upholding ideals of openness and transparency better than other system of governance, this must be publicly displayed and publicly defended; otherwise it is only an illusion of transparency. Accordingly, it is unclear whether contemporary responses to cyber issues (e.g. crime and deviancy) handled via 'Big Data' policing efforts, reflect the Canadian public institutions' ability to be adaptive, creative and flexible to contemporary social transformations of the Digital Age without sacrificing the privacy of Canadians.

Voluntary disclosures allow the private sector to hand over metadata to police and national security without a warrant and absent of judicial authorization. As Geist (2014a) argued in Committee debates, metadata is so sensitive, it can "reveal political affiliation, religious practices, and people's most intimate associations...aggregation of telephony metadata—about a single person over time, about groups of people, or with other datasets—only intensifies the sensitivity of the information" (5). Fraser (2014) also noted in Senate debates on C-13, that the GoC has maintained that metadata and "phone book information" are analogous and police therefore do not need to be subject to any formal requesting procedures (22:36). As Escudero-Pascual and Hosein (2002) have highlighted, the regulatory environment surrounding policy formations calling upon a need for greater law enforcement access to user metadata information is often wrapped using technology-neutral language. Their findings are further confirmed through the analysis of discourses surrounding Canadian lawful access deliberations. Indeed, as Mackay (2014) contended

in the House, lawful access is "about modernizing [the law] in a way that takes Criminal Code sections from the age of the rotary dial phone into the 21st century, the Internet age" (8113). Rhetoric is thus preceded by assumptions that C-13 modernizes law, but it places the sensitive issue of cyberbullying at the fore to legitimize these policing security policy shifts under the presupposition of maintaining public order and protecting 'society'. This rhetorical technique positions rotary dial phone information as being analogous to routing information of Internet communications protocols.

Indeed, as MP Goguen (2014) argued in House debates, Bill "C-13 would amend certain definitions found within the Competition Act to ensure that they are clear and technology neutral and that they align with those in the Criminal Code" (8511). What is more, when MP Péclet (2014) proposed to change the lower legal threshold for obtaining user metadata proposed by Bill C-13 from 'reasonable grounds to suspect' to 'reasonable to believe' (3), MP Dechert (2014) argued, "reasonable grounds to suspect is a common standard. It is used in many similar provisions in the *Criminal Code,* including with respect to *telephone data.* Therefore, we think it's completely appropriate that it be the standard in this case" (emphasis added, 4). As Escudero-Pascual and Hosein (2002) have argued, technology-neutral policy is invoked under the assumption that technologies are continuously changing, therefore it may "ensure that new laws do not need to be passed every time a new technology is invested. However, technology-neutral language may be used to ignore, willful or not, the challenges, risks, and costs to applying powers to different infrastructures" (68). For instance, as MP Hoback (2014) had argued on lawful access, "Previously, a telephone number may have revealed the identity of a suspect; this information may now be found in the transmission data of an email" (4573). Still, this

inquiry overlooks the more sensitive elements inherent to metadata transmission versus older, traditional telephone systems that may only reveal the caller, receiver, number time and the date. Meanwhile, the metadata, as previously discussed, can provide a plethora of intimate information where there is no functional equivalent to the telephone data. As MP Marston (2014:7668) argued in regards to the vast Snowden disclosures, "When we talk metadata and improper access, he has released to the world thousands upon thousands of examples of where metadata has been abused and put into the wrong hands". Therefore,

> Perhaps with bullying, [the Government] is something like a magician. A magician distracts with one hand and picks pockets with other. We are very concerned that [C-13] is opening a door to allow access to data that is well beyond what anybody would understand is necessary to help prevent bullying. That distraction is very concerning (ibid).

Statements by MP Elizabeth May (2014) in Committee debates also reflect such rhetoric around the Government's sleight of hand. She argued that, "It isn't at all about combating cyberbullying. It is something of a different character altogether in the guise of protecting children from Internet crime and predators. It's a clever disguise, but behind that disguise is Big Brother" (5). Ultimately these practices contest the prevailing state assumption and narrative, which presupposes that lawful access law is required for police to "do their job properly" and that these new legal measures "do not infringe upon Canadian's reasonable expectations of privacy" (MacKay 2014). Despite the dystopian narrative outlined above, our hope should not be lost and the trajectories of policing aspects of surveillance are not deterministic by any means. Ripples of change, ebbs and flows can always persist.

5.4 *R. v. Spencer 2014,* unanimous decision but uncertain effect

R. v. Spencer [SCC:2014] set high precedent for contemporary understandings of anonymity online and police investigation tools. The background to this case states that in

2007, Deputy Sergeant Darren Parisien of Saskatoon Police Criminal Service Intelligence Section discovered child pornography files shared on the popular file-sharing networking site, LimeWire (paragraph 7-10). An IP address was identified but the identity of the user was unclear. At the police officer's discretion, Parisien contacted Shaw Communications, a TSP/ISP in Canada, to voluntarily obtain the user's basic subscriber information (BSI), which includes the name and address of the suspect (identified later on as Matthew David Spencer). Following Shaw Communications' disclosure, Spencer was charged with being in the possession of child pornography and with distribution of child pornography.

At the lower provincial court, he was convicted of being in the possession of said data, although he was acquitted on the distribution charges, as the trial judge was unable to establish the *mens rea* component for the criminal act. Principally, this was due to the fact that the defendant did not *reasonably* know LimeWire allows other users to access materials on a user's shared file drive (paragraph 3). Larger issue remained as to whether the police breached Spencer's Section 8 *Charter* right, as his BSI was obtained absent of any judicially authorized warrant therefore argued to constitute an "unreasonable search". At Saskatchewan's Court of Appeal, the defense was dismissed and the judge dissented, "there is no reasonable expectation of privacy in the information attached to the Internet protocol address that had been obtained by the investigating police officer directly from the Internet provider without a warrant" (paragraph 2). This decision was contested and Spencer's case proceeded forward to the Supreme Court of Canada in summer 2014.

At the Supreme Court level, the judges' dissent departed markedly from the lower court trial judges and established landmark precedent for online privacy. Concluding,

> In the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. The disclosure of this

> information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search [66].

Geist (2014c) has provided detailed analysis on this decision. In particular, he notes that this case establishes that TSPs/ISPs can no longer disclose user metadata to the police or national security agencies absent of a warrant except for under an exigent circumstance[61] prescribed by Law. In theory, this decision should now end the bulk metadata collection known to have occurred, as described at length in the previous sections of this chapter. When debates in the House proceeded on C-13, MacKay (2014) summarized the *Spencer* case, "It talked about the fact that people have a reasonable expectation of privacy when they go online", noting, "I do not know whether all Canadians actually believe that when they go online" (8110). In addition to his interpretation, he argued, "the Spencer decision does *not* require amendments to Bill C-13" (emphasis added, 8109). In concluding Senate debates, Senator Mobina Jaffer (2014:2580) commented on the critical fact that lawful access was not amended to account for the *Spencer* decision, arguing,

> The minister has not even started to look at our report. He has not even acknowledged that he has implemented any of the things we said in our report. It's not about a Senate report. We know that the government does not implement many Senate reports… My worry is that, again, this will go to the courts and, again, the pain of our children will continue[62]... Honourable senators, before you support this bill, I ask you to think about the children in your community who will not be helped by this bill.

---

[61] "Exigent circumstances" is defined as being "imminent danger of the loss, removal, destruction or disappearance of the evidence if the search or seizure is delayed" (*R. v. Grant*, SCC:1993, para 32). In the context of warrantless wiretapping these conditions can be justified under Section One of the *Charter of Rights and Freedoms*. Although, the person(s) subject to a wiretap must be notified of this action (see *R. v. Tse,* SCC:2012).
[62] Nova Scotia's *Cyber-Safety Act* (2013), which was enacted in the wake of Rehtaeh Parson's death, was sent back to the provincial legislature in August 2015 after the Supreme Court determined that certain elements might violate the Charter (CBC 2015).

Given the Conservative's frequent challenging of Supreme Court decisions, it is unclear how lawful access will proceed in terms of the tools it has afforded given that it received royal assent and was unadulterated from its initial proposal. It is also unclear if voluntary disclosure practices proceed pre- or post-*Spencer* decision and what degree the Courts or external bodies examine such practices, especially in light of non-reporting and problems known to exist in the 'independent' reviews of policing and national security agencies. Given that certain agencies, such as CSIS, are 1) only subject to review *after* activities are carried out rather than having an internal oversight mechanism, and 2) the reviewing bodies are not privy to unfettered records access due to the highly sensitive nature of their work[63], it is questionable whether these agencies will be held to reasonable standards to ensure there is adequate compliance with the Law. Equally, it is uncertain if PIPEDA will be amended to become "a statute whose purpose is to increase the protection of personal information" rather than to do its opposite [*Spencer* SCC:2014]. Indeed, as Geist (2014a) noted in debates on lawful access, ISPs/TSPs disclose "more than just basic subscriber information" when facilitated by PIPEDA, as the law "is so open-ended, *content* can also be disclosed voluntarily, as long as it does not involve interception…[it] is by no means limited to basic subscriber information" (emphasis added, 7). Brief examinations of other laws recently passed within the security and order maintenance pipeline also demonstrate there is ample evidence to suggest that privacy-safeguarding barriers are being breached.

---

[63] Public Safety (request #A-2012-01994) records have defined "sensitive information" as "information relating to international relations or national defence or national security that is in the possession of the [GoC], whether originating from inside or outside Canada, and is of a type that the [GoC] is taking measures to safeguard…sensitive information does not require proof of harm in order to come within the definition" (97).

Under Canada's present regime, policy prescriptions introduced seldom have the positive effect of generating greater privacy protections or for restraining powers of law enforcement and national security agencies. Indeed, citizens have witnessed the opposite with initiations of additional mandatory minimum sentencing, permitting CSIS agents to defer *Charter* rights upon judicial authorization by a court (with C-51) and other invasive tactics or strategies (Forcese and Roach 2015). In the contemporary climate of voluntary disclosures, combination and introduction of other yet-to-be-assented Acts may advance to exacerbate issues of civil liberties and the concerns highlighted herein this Chapter.

It is often said that social scientific inquiry and 'life' does not operate in a vacuum. Accordingly, while lawful access, Bill C-13, has loudly signaled a number of alarms and has remained the primary focus of this research, its ominous tone deepens in the context of other enactments and proposals. For instance, Bill S-4 or the *Digital Privacy Act*[64] put forward by Industry Canada's Minister, James Moore, triggers other compounding issues when depicted next to C-13. If enacted, this Bill will allow private corporations to share information held in private sector databases with other corporate entities absent of user consent and absent of any notifications of the happenings. As Geist (2014d) argues, Bill S-4 proposes to permit organizations to disclose personal information (not just metadata) absent of court review or consent upon the individual for purposes of "investigating a contractual breach or possible violation of any law" (N.P.). In this way, if an individual voluntarily shares their information with a single corporation, other entities can be privy to that data. This raises important privacy-related questions regarding personal medical

---

[64] Official name of S-4 is *An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act*.

records disclosed to private insurers, sharing of metadata telephony information stored in a private database and the seemingly innocuous consumer reward points programs that highlight user spending habits. As noted in discussions around intelligence-led policing and predictive analytics in Chapter 3, disparate (meta)data might not embody significance or illuminations on its own. Yet, when its treated and combined with other aggregate data points, a 'picture' can emerge to carry on added significance that may not otherwise have produced such a comprehensive puzzle from the distinct pieces observed in their solitude.

The implications for Canadian autonomy and for other civil liberties are profound when we consider that: 1) under section 7(1) of PIPEDA, personal data can be collected *absent* of the user's consent or even knowledge; 2) tenants of C-13 updated the *Criminal Code* to add S. 487.0195(1) and (2) to give immunity to persons that disclose data to third parties, as long as the disclosures is permitted by the law and yet those who conduct the disclosure do not need to meet any requirements of "good faith" or "reasonableness" as articulated elsewhere in the *Criminal Code* under Section 25; and 3) that Bill S-4 would update PIPEDA to allow information sharing and data duplication across organizations in cases of potential contractual breaches or for the purposes of investigating *any* potential violation of law by adding the new, prospective Section 7(3)(d.1).

The Canadian Privacy Commissioner, Daniel Therrien (2015), noted the provision and amendments forwarded within Bill S-4 lowers the threshold of disclosures, arguing it

> Open[s] the door to widespread disclosures and routine sharing of personal information among organizations based on a hypothetical risk…this could lead to fishing expeditions to obtain information about individuals based merely on suspicion. Moreover, once the transparency of the investigative body regime disappears, there will be no mechanisms to identify which organizations personal information is being disclosed or to determine for what general purpose based on their mandate (N.P.).

In regards to *R. v. Spencer*, Therrien noted there is still significant amount of ambiguity relating to practices of voluntary disclosures. Organizations are uncertain when or if they can make warrantless releases. To this end, he observes TSPs/ISPs have varying standards where some require a warrant, others continue to disclose absent of a warrant; operating in the frameworks of the pre-*Spencer* decision. Consequently, Therrien has called for greater clarity regarding PIPEDA; though his recommended changes have not yet been enacted in law and might never be. Meanwhile, his call for better transparency in reporting aspects of metadata disclosure practices by corporate entities is not a legally binding article[65].

5.5 A New Way Ahead

The Internet is oft conceptualized as being a decentralized virtual space whereby hierarchies of authority and control are eliminated (Hands 2011:82). It is referred to as a *technical commons* or *information commons*, conjuring up images of open-access and of public ownership (Lessig 2001; Kranich and Schement 2008). These narratives position the Internet redolent of an Agrarian Society; a period romanticized and bolstered by ideas of freedom. As an internal, backstage CSIS document (request #A-2012-248) remarks,

> A more connected world certainly has benefits, but it is also harder to assess and secure. We have a great challenge before us. The Middle Ages was an age of competing powers and influences in Europe, with the church and aristocracy competing relentlessly. There was no single or preeminent power or structure. This diffuse understanding of power seems very relevant today. However, unlike the Middle Ages, we have significant institutional structures to help govern this complexity (34).

---

[65] Rogers Communications recently released their first transparency report to represent 2013. It shows 174,917 requests were received. Meanwhile, the report for 2014 indicates 113,655 requests were received but *warrantless* requests stopped in June 2014, which interestingly coincides with the Supreme Court decisions made in *R. v. Spencer* [2014].

This chapter demonstrates there are multiple actors making the Internet a governable or governed space (see also Mopas 2009). This shift has predominantly taken place through rhetoric that endorses policing policy changes or development of law vis-à-vis utilitarian arguments. Present directions within the productions of security raise flags of concern for MPs, academics, experts and the public for lawful access' perceived and real effects on the lived realities and personal autonomy of Canadian citizens.

The Internet is an environment to "voluntarily connect with others around culture, ideas, and tastes" (Kee 2011:426). It creates space(s) and "new forms of association not rooted in family, rank, or vocation" (Wilson and Yachin 2011:1). It has produced new "publics" to help combine "a variety of 'public spaces' in their action" (Iveson 2008:13). Internet publics and new technologies that permit connectivity may in fact "not only lead to new arrangements of people and things" but also "new forms and orders of causality and, indeed, new forms of knowledge about the world" (Akrich 1992:207). The making of publics arises from the collective efforts of a community that "inscribes" a particular purpose or vision for how a space—or new technology—will and can be used (208). Still, users can help develop "new practices and applications", which positions them as a being "designer"; we can repurpose this 'Third space' of the Internet or technologies for new uses not initially imagined by its original developers or creators (Georgieva 2010:1). The Web therefore facilitates a variety of social activities, but it has also allowed policing and surveillance activities to (re)emerge and perhaps even flourish. Still, we can equally use

technologies to circumvent these practices and to garner support to make a change in the law, of which can partially mute or render moot some these activities if we so choose[66].

Still, the Internet's openness situates it as being an environment, which is equally "ripe for exploitation and enclosure" (Hands 2011:79). Notoriety of the Internet is that it is considered a part of the public domain; it is a *virtual commons* (Lessig 2001:56). Yet much like the enclosure of the commons in 16th and 17th century England, public-private actors are similarly enclosing the Internet. In England, (re)appropriation of land gave rise to the Diggers, Levellers, and Ranters, who argued, "Freedom was limited to those who lived off their own accumulated wealth or worked for themselves" (Levy 1983:116). The enclosure and reclamation of the Web as a governable space, has given rise to collectives like WikiLeaks[67] and Anonymous[68]; contemporary defendants of the Internet. Proponents of cyber autonomy and defendants can therefore use the Internet and other ICTs to create 'infrastructures of resistance' (see Shantz 2013) of state and corporate appropriation and manipulation of these earlier ideals of the Internet. This is of course, an effort to maintain previous sequestrations that occurred, as the Internet's origins and roots are attributed to American military exploratory constructs (see Hafner and Lyon 1996).

'Big Data' surveillance presents us equal parts promise and challenge. Police have used Big Data to help predict the occurrences of where burglaries are most likely to exist,

---

[66] The House of Commons passed MP Kennedy Stewart's (2014) private member's bill M-428, which allow the government to receive electronic petitions. If this bill receives royal assent, one of its tenants is that if a petition receives 100,000 signatures within 90 days debate would occur within parliament on the matters of the petition for a period of 30 minutes. In this sense, Canadians would be able to engage in more directly democratic processes by using the technologies at their disposal by crowdsourcing or harnessing the powers of the Internet to support and protect its important essence in every day life.
[67] WikiLeaks is an international organization that publishes information anonymously.
[68] Anonymous is a decentralized, international hacktivist (i.e. hacker-activist) collective.

reducing rates of incidents (Joh 2014). Metadata from cellular devices has also illustrated whether a person(s) were in proximity of a particular area based on wireless network data sent *to* and *from* a digital device to a radio tower; that is, metadata can disrupt a suspect's alibi if we are in possession of technologies (Young 2004). Presently, Big Data's use by police has been more effective in post-criminal event investigations by amalgamating and by analyzing the disparate points of data from variety of sources (McGarrel, Freilich, and Chermak 2007). As Pozen (2005) argues, triangulation of public and privately available data can be used for proactive policing purposes,

> Disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information. Combining the items illuminates their interrelationships and breeds analytic synergies, so that the resulting mosaic of information is worth more than the sum of its parts. In the context of national security, the mosaic theory suggests the potential for an adversary to deduce from independently innocuous facts a strategic vulnerability, exploitable for malevolent ends (630).

Canada's Privacy Commissioner (2013:7) demonstrates using multiple case studies, that metadata, which can be obtained by the police "without prior judicial authorization", can clearly "provide a starting point to compile a picture of an individual's online activities; including: online services for which an individual has registered; personal interests, based on websites visited; and organizational affiliations". As the Commissioner's report notes, it was the innocuous determination of a single IP address that became "the starting point for an investigation [into] the widely-publicized Petraeus case in the U.S." (6).

Big Data surveillance challenges contemporary understandings of 'privacy' when used proactively by policing assemblages to make known the public activities in absence of oversight. As Spratt (2014:10) argued in Committee debates of lawful access,

> It's not an answer to say that if you have nothing to hide, you should be willing to give this information over…Privacy is not about hiding. Privacy is about a person's right and ability to control the information about them and their freedom of choice…it's a misnomer to say that [Bill C-13] makes it clear that this is just subscriber information, i.e., name. That's not what is says. It's the type, duration, time, size, origin, destination, and determination of your data and anyone else's data.

Despite such powerful statements and defense of personal autonomy, others maintained in lawful access debates, "The right to remain anonymous cannot take precedence over the basic right to feel safe and protected" (Anderson 2014:3). MP Dechert (2014) argued, "C-13 introduces a number of measures to take the mask off the perpetrator" of a crime (7674), but equally this can threaten contemporary understandings of privacy, of which is a fleeting currency today as we pay for online services *with* our personal data (Soghoian 2012). As the Government of Canada continues to find a "new way ahead" (Gendron and Rudner 2012) to police and to keep watch, law enforcement and national security need to appropriately balance public safety activities with the civil liberty needs of citizens.

5.5.1 A Fishing Expedition?

Spratt argues (2014) that "the real concern is that the expansion of police power and limiting liability for the party agreeing to disclose will result in increased police fishing expeditions, and of course we have seen from some reports some very alarming information about current practices in that regard" (4). When it comes to using metadata to police, the GoC must ensure practices are narrowly tailored to criminal investigations, as Butt (2014) noted, "It cannot be a fishing expedition" (9). After examining official and unofficial discourses and records, it is clear that policing practices have not always been narrowly tailored. Fraser's (2014) comments in Committee capture this genuine concern,

> What I am concerned about, and think Canadians should know, is how often information about Canadians is obtained, with or without a warrant, that

> never in fact leads to charges…Maybe they're getting information about a huge number of people, such that in fact it amounts to fishing expeditions whereby they're going to catch a couple of bad guys, but it's too much (13).

As MP Toone (2014) alluded to in House of Commons debates, there is a possibility for lawful access to produce surveillance structures reflecting a "fishing trawler", which will "suck up all the information as it goes along" (8537). It is unknown if Canadian police forces are engaged in a form of widespread clandestine surveillance occurring elsewhere such as in the United States (Greenwald 2014). Still, it is evident Canadian police forces predominantly regard ILP models to improve surveillance tactics. Couple this fact with the variegated potentialities of 'Big Data'; future implementations outpace contemporary imagination. MP Borg (2013:1521) argued therefore that lawful access legitimizes,

> An online spying program free of any oversight...after hearing about the U.S. scandal and the American people's surprise at learning what was going on with Verizon, the NSA and PRISM. The government is recreating a very similar system in a bill that is supposed to address only cyberbullying.

Sheptycki's (2004) work shows, "[ILP] predicated on widespread system surveillance has a tendency to demand 'more data' rather than 'better data' or better *data analysis* when problems are identified" (316). If we accept this argument, one implication of this is that the police could follow up on users whose metadata has revealed particular keywords or connections deemed to be suspicious based perhaps on political or partisan reasons. Yet, such practices would ignore the unpredictability of social life; which is to say that no amount of data collection or data analysis could curtail most or all criminal occurrences in any society (be it physical or virtual). Jason Young (2004:48-47) makes an important remark in this regard around initial debates and iterations of lawful access in Canada,

> In the present political atmosphere and in the context of the *Lawful Access* proposal, it does not take much foresight or even creativity to interpolate 'driving' with 'surfing' and 'Black' with 'Muslim' to imagine that reduced

> judicial scrutiny could lead to a new cyber-offence, in Canada, of "Surfing While Muslim". Salient interests could include a Muslim-sounding name, an IP address from an Arab country or organization, an online purchase of the most recent book by author Irshad Manji, Salman Rushdie or any number of others as defined by the personal biases of the individual investigator.

To this end, Internet users could use the web browser Tor, for instance, to circumvent and distort the records of certain metadata points such as an IP address, websites visited, and the respective time and date of activity. Nonetheless, there is little, if any ways, to hide the fact that the user is using the Tor browser. Given that Tor is often used by journalists, academics and those concerned with privacy, it is easy to deduce that this web browser could be socially constructed as being 'suspicious' (see Tsoukala 2008). In one *Access to Information* record regarding the use of the Internet by extremists or terrorists from CSIS (request #A-2013-168), CSIS argues, "Radicalization is defined as the process through which an individual or group moves from mainstream, socially acceptable beliefs and activities to those which exist on the fringes of society and are increasingly unacceptable" (62). Given the fact that Tor, for instance, is a means to connect to the Web outside of regular use, as most may be more inclined to use the likes of Safari, Firefox or Chrome to 'surf' the Web, policing and national security agents may hone in on these users; seeking to obtain perhaps a production order to get additional access to their online activities, of which is of course a reflection of our offline selves. That is to say that user metadata is redolent to a 'data double', which is "the multiplication of the individual, the constitution of an additional self" (Poster 1990:97 as cited in Haggerty and Ericson 2000). Our data double and displays of 'fringe' metadata may then open up users to targeted intervention and scrutiny. Metadata might allow policing agents to focus on users via an intelligence-led approach that presupposes and argues 'X and Y' is suspicious for 'A and B reasons'.

As Haggerty and Ericson argue, "In this process, we are witnessing a rhizomatic leveling of the hierarchy of surveillance, such that groups which were previously exempt from routine surveillance are now increasingly being monitored" (ibid) by an additional medium. This medium—the Internet and our metadata—provides yet another way for the state to access personal artifacts (e.g. Web browsing habits and therefore interests), which would not be available otherwise except where a warrant existed for this 'surveillance' or in-person interrogation following specific procedures. Given statements made by Michael Hayden (2014:N.P.) stating that Americans "kill people based on metadata", it is not hard to imagine a case where Canadian policing agencies one day proactively detain and arrest individual(s) based on their metadata telephony information, which one could be charged with Sections of the *Criminal Code* around conspiracy. As another unofficial, 'backstage' record by CSIS has noted, (request #A-2013-133:10), "When you access the Internet you leave traces (history files, favorites, cookies)…ask yourself: who will have access to this information I am posting? What controls do I have over how this information is used?"

5.5.2 Minority Report Creep?

As Verfaillie and Beken (2008) have argued, failure to consider this could lead to a society much like the film *Minority Report*[69] (2002), where police and national security agencies conduct routine arrests on citizens under the auspices of crime prevention (via some pre-crime unit) on account of some perceivably objective statistical figures. This is important to bear in mind, as law enforcement agencies adopt an intelligence-led policing

[69] *Minority Report* is a sci-fi film set in the year 2054. It chronicles a futuristic police department called "PreCrime", which specializes in apprehending suspects before they commit criminal offences based on intelligence provided by three individuals that can predict the future and communicate their visions through sophisticated technologies.

paradigm, which presupposes, "threats must be countered and suppressed *before* they are imminent" (Gill 2006:44). Indeed, the GoC has already made possible such "Orwellian" possibilities. As Larsen (2008) has revealed through his use of the *Access to Information Act*, documents reveal, "The Immigration and Refugee Protect Act [IRPA] empowers the state to indefinitely imprison without charge or trial, and on the basis of secret intelligence, those non-citizens it deems to represent potential threats to national security" through issuance of 'security certificates' (21). Larsen notes, "In practice, [this] can mean a prolonged, indefinite term of imprisonment on Canadian soil, described by the government as a 'preventative measure'" (ibid).

Conspiracy under Section 465(1) of the *Criminal Code* comparatively permits the police to recommend charges to the Crown based on reasonable evidence that a person(s) has conspired to commit a summary or indictable offence; that is, it is a crime prevention function or an issuant perceived to delay certain harm. The uses of Big Data surveillance, however, exponentially produce more measures for police to proactively intervene in the activities perceived to be somehow malevolent. Still, it is important for policing and for security intermediaries to realize ILP via Big Data cannot positively ascertain what will happen; it can only assess potential likelihood of occurrence (Verfaillie and Beken 2008). Yet, it is a matter of subjective interpretation. This is to say, agencies should be cautious when policing or keeping watch by way of positivist paradigms, which often (mistakenly) suggest, "knowledge comes in the form of numbers" (Mopas 2014:4). Numbers—like metadata—can never be objective, impartial, impersonal or all complete.

As Rallis and Rossman (2012) have argued in relation to social scientific inquiry, information is always "partial, incomplete, and context bound" (50). In using statistics for

calculating the criminal risk or likelihoods, there must be assurance that the quantitative policing and surveillance methodologies contain equal oversight around the actual legal thresholds for obtaining user metadata. Otherwise, there runs a real risk of legitimizing draconian bulk metadata collection or broad, sweeping interpretations of law. As Edward Snowden (2015) argues, "Once you grant the government some new power or authority, it becomes exponentially more difficult to roll it back. Regardless of how little value a program or power has been shown to have " (N.P.). This argument can be applied within the context of lawful access in Canada, which reified *previously* occurring police action.

It can be deduced that Big Data surveillance will continue apace in Canada, as the police only begin to find varying potentialities that can be derived from these constructs. Once any one of Canada's mosaic of agencies involved in the production of security can empirically and demonstrably justify Big Data's usage, it is assumed that these power and the access to the troves of user metadata abound in private servers will only increase as a result. Where warrantless access to metadata may only presently be permitted for exigent circumstance, this exception may one day become a normalized state of affairs (Agamben 2000). What is arguably missing from these contemporary and recurring debates is what the optimal and acceptable level of crime is in Canadian society—both online and offline. The Government of Canada must ask itself this question and to what end they are willing to go to in order to detect or to prevent crime, terrorism and deviant activity in every day life. The Government of Canada must be committed in an open and transparent manner to provide evidence that such security measure(s) work and are cost beneficial and ethical in a liberal democratic secular society.

We are putting at risk people who might want to use the Internet to challenge the government or its choices and policies. We are putting the Internet at risk as a free and open medium. With regard to Internet surveillance and online spying—no matter what we call it—we cannot allow our Internet to be destroyed by these sorts of provisions. It is extremely important that privacy remain paramount in Canada. This is entrenched in section 8 of our Canadian Charter of Rights and Freedoms. It is paramount that this right always be respected.

– MP Charmaine Borg (2013)

6 Conclusion

Computer and network surveillance activities have proceeded in quite opaque and unaccountable formats by Canada's mosaic of policing and national security community. Structural secrecy has dominated the every day practices within these actor-networks that deliver surveillance activities to the extent that policing, *done digitally*, is afforded only through the reliance and compliance of corporate-led telecommunication carriers. State-sponsored Internet access is atypical and unfound in Canada. Perpetuation of state power over the digital lives of Canadian citizens cannot therefore transpire except for under the circumstances and the partnerships that have permitted state departments to be 'enrolled' within the mechanism of a corporate-public lens. The insurrection of lawful access bears a plethora of concerns for privacy, information control and data-sharing agreements. This is to say that intelligence-led policing paradigms in the context of the Internet oft emerge *through* private networks that are enveloped in opaque systems, which ultimately reduces accountability, recording keeping and regulatory oversight of public law enforcement and national security agencies that will continue to be watchers of the Internet.

In democratic confines of governance, a multitude of checks and balances exist to ensure power within the state—as well as among other corporate and personal entities—do not sway to the detriment of any other integral structures. Increasingly, our public and private spheres are colluding at the intersections of technology and of debates around the

tenability of the Internet. In this vein, how the Government of Canada balances activities of security with the qualified rights to privacy of citizens will determine the boundaries of social, political and economic life moving forward. It is not adequate for the state to now claim that offline and online activities are *distinct* from one another and therefore *Charter* rights should only apply in the former context. The citizens of Canada—of the Internet—need to appreciate that the Internet is a contested space and that engagement is required to ensure rights are upheld, noticeably articulated and legally-bound in yet-to-exist policy prescriptions (see MacKinnon 2012). It is not enough to readily point out these problems. Citizens must be active: build infrastructures of resistance (see Shantz 2013); circumvent surveillance through virtual private networks and end-to-end encryption; create or join an organization(s) that actively campaign for restraint of state and corporatized surveillance; engage and debate ideas of Internet self-governance (see Barlow 1996); and contemplate the makings of a 'Digital Magna Carta' to engrain netizen rights (see Berners-Lee 2012).

Openness and transparency are two mores woven into the very fabrics of Western democratic societies and each are reflected within numerous provisions, constitutions and charters. To the extent that Canadian surveillance and policing activities drift away from these centralities, potentialities of abuse can become unrestrained and the exercising of proportionalities of control can become unhinged. This is to say that where the *activity* of Internet policing and surveillance becomes facilitated *through* private networks, openness and transparency becomes opaque due to the inherent nature of corporate structures. With this in mind, regulatory state bodies can still mandate many changes to present 'standard operating procedures'. Still, it requires the activation by 1) state representatives engaged in the policy enactments, 2) public participation that raises awareness, 3) judicial review

and dissent, or 4) the volition of private-led actors that perpetuate and sustain systems of secrecy for these practices. Restricting the watchers and protecting privacy is possible[70].

This thesis has been primarily concerned with exploring the emergence, rehearsal and performance of discursive enactments that contributed to the reifying lawful access in Canada. It aimed to elucidate on *why*, *how* and *with what effect* policing and surveillance trends of lawful access were established to 'secure' the cyber environment from official (front stage) and unofficial (backstage) vantage points. It explored social constructions of this framework, which has legitimized policing powers for law enforcement and national security communities. This study explicated questions through two dialectical positions of official, 'front stage' discourses and the unofficial, 'back stage' discourses by drawing on the dramaturgical metaphor of Goffman (1959), ideas of 'open-government activists' (Walby and Larsen 2012; Piche 2012; Geist 2014; Parsons 2014), internal state records generated using Canada's federal *Access to Information Act* and transcripts from multiple stages of legislative debates surrounding the evolution of lawful access.

Specifically, I have challenged to answer calls by Parsons (2015) to create "more context about dimensions" of the domestic surveillance and policing "puzzle" in Canada (16). This study also attempted to make connections to other scholarly findings of lawful access debates, which are commonly enveloped via 'technology-neutral' language, which may have devastating consequences for privacy due to either deliberate or unintentional tenets written into ambiguous or technology-unspecific tones (see Escudero-Pascual and Hosein 2002). Debates emanating around lawful access in House of Commons debates

---

[70] Marcon (2015) notes, "We can only wait. But not for long, and certainly not idly. The potential to seize, to act, to engage is always before us" (116).

and Committee hearings were largely characterized by anecdotal evidence calling upon a greater need for powers for those involved within the production of security rather than establishing the clear lack of powers absent for police (Young 2004). Indeed, as evidence from *Access to Information Act* records has demonstrated, law enforcement agencies have carried out widespread surveillance efforts for over a decade via corporate TSPs/ISPs that facilitate troves of voluntary user metadata disclosures. To this degree, I argue Canada's lawful access was assented into law to legitimize (i.e. retroactively legalize) previously occurring policing activities. Although, in doing so, lawful access also created provisions to protect and insolate third parties from incurring any criminal or civil liability when a disclosing data is made whereas the rescinding of this information also no longer requires measures of "good faith" and "reasonableness" to be met, as articulated elsewhere under Section 25 of Canada's *Criminal Code*. With this in mind, its hypothesized that metadata disclosures will increase in scope once *any* department involved in the 'securitization' of the Internet can empirically and demonstrably justify these powers of engagement in the course of proactive, intelligence-led policing practices.

Above this, I have raised critical questions around the legality of prior policing practices in Canada, as the RCMP have admitted to engaging in "general policing duties" on the Internet in cases where "no criminal offence is under investigation" (Public Safety Canada request #A-2012-00113:39). Ability to carry out such activities was facilitated by voluntary disclosures by TSPs/ISPs, as judicially authorized warrant would not have been given without a formal investigation. To this extent, these practices transpired due to the tenets embedded in the *Personal Information Protection and Electronic Document Act* (PIPEDA), which requires a voluntary disclosure to be made for "purpose[s] of enforcing

any law…carrying out an investigation…[or] administering any law of Canada or a province" under paragraph 7(3)(c.1). This is cause for concern as evidence suggests that TSPs/ISPs should never have facilitated these disclosures under PIPEDA. In similar vein, the RCMP may have (unwittingly) provided false pretenses, which led to the disclosures for cases where indeed no criminal offence was under formal investigation. In answering these queries, it is plausibly a combination of these deductions; though given the lack of effective data documentation practices such answers cannot be ascertained without more investigation into this issue, which exceeds the scope of this thesis.

Towards a symbiosis of private, corporate-led networks that facilitate surveillance aspects of policing for public agencies, this thesis contextualizes works of other scholars who have documented existence of what I refer to as *pay-per-view-disclosure* systems. In this vein, not only have Canadian ISPs/TSPs allowed these practices to flourish by being the 'keepers' of Canadian subscriber data, they have repeatedly sold Canadians' metadata to policing agencies for a sum between $1.00 and $3.00 (Geist 2014). Beyond this, I have discussed the compounding effects of lawful access (C-13) when placed with other Acts, such as Bill C-51 (the Anti-Terror Legislation) and Bill S-4 (the Digital Privacy Bill).

6.1 Recommendations

The Government of Canada has taken significant steps toward 'securing' the Web through the tenets of lawful access. The ability to now detect and to preempt deviant and criminal activity has strengthened, as law enforcement and national security partners are afforded with *legal* policing and surveillance powers. Moreover, ability to share data and to prosecute those outside of traditional zones of jurisdiction have now become unhinged, as lawful access has brought along new means to engage in broad mutual legal assistance

provisions with other foreign nation states that have also ratified the Council of Europe's *Convention on Cybercrime* (2001). Still, the following action items are recommended:

1. Establish an *Internet Policing and Surveillance Oversight Act* which:

    - Requires monthly reporting on the frequency and purpose of formal and voluntary request made by law enforcement and national security agencies
    - Mandates that TSPs/ISPs keep records on formal and informal requests
    - Establishes independent, non-appointed members to analyze incoming information on an ongoing basis to ensure agencies are compliant with articulated legal statutes, Acts and judicial decisions (e.g. *R. v. Spencer*)
    - Mandates TSPs/ISPs disclosures to policing agencies be encrypted to help reduce unwanted capture of sensitive subscriber information
    - Establishes clear data retention policies for TSPs/ISPs to limit the amount of longitudinal information that can be captured and disclosed
    - Creates compulsory reporting to subscribers if user data is handed over to a third-party while including an exact record of the data that was disclosed

The establishment of such an *Act* would assist to breach some existing degrees of opacity in the performances of policing and surveillance conducted through third-party, corporate entities. This would place an onus on the corporate structures, treating them more like a public body rather than a legal, private person insofar as they deliver us public services: policing, cyber securitization and electronic surveillance.

This thesis scratches the surface of the 'prism' that houses emerging policing and surveillance trends in Canada. It illuminates the troves of third-party assisted metadata telephony disclosures, the implications of intelligence-led policing paradigms and some of the consequences of security policing policies that have expanded proactive, Big Data surveillance efforts to keep watch on the Web. Beyond the surface of this prism, there are a number of areas for future inquiry. No doubt has this project raised more questions than

it has attempted answered. Yet, inquiry into these subjects and various sides of the prism become hindered due to the inherent dispersion mechanisms that prevent more in-depth penetration into the angles presented to the 'front stage'. This is to say mechanisms such as Canada's *Access to Information* and *Freedom of Information Act* can provide 'partial entrance' (Walby and Larsen 2012) into the manifest backstage of federal or of provincial activities, respectively. However, public understanding is still subject to the partitioning of actors and statutes activated to restrict how agencies operate within their legal powers. While *Access to Information* and *Freedom of Information* Acts exist to offer requesters a concession to witness rehearsals take place in the backstage, the 'viewing pass' is limited and the gaze is always partial and obstructed. In this vein, given the project's emphasis on *Access to Information* records, arguments may gain attention of certain Government of Canada departments examined herein therefore prompting a response to this work, which may hopefully open up a more nuanced or publicized discussion.

The same powers that allow entry to the hidden side of the backstage, beyond the curtain, are the exact same powers that allow for redactions within *Access to Information* disclosures. One method to enhance public understandings of backstage activities would be participation of actors to come forward and register their voice (Soghoian 2012). Still, a methodological approach to establish trust and facilitate open dialogue is non-existent and no doubt restrained due to the private nature of government work and non-disclosure agreements employees must abide. To this end, it is perhaps only vis-à-vis an unrelenting position of internal leaks and use of *Access* to *Information* requests that Canadians can be provided with compounding evidence to shine the light on the opaque prisms of security, policing and order maintenance activity to bend toward justice and vindicate contention.

Bibliography

Alexander, Jeffrey. 2004. "Cultural pragmatics: social performance between ritual and strategy." *Sociology Theory* 22: 527-573.

Anonymous. 2012. "Anonymous – Our Warning to Vic Toews & the Parliament of Canada". Youtube: https://www.youtube.com/watch?v=OyOQFYeBIho (accessed on March 29, 2015).

Andrejevic, Mark and Kelly Gates. 2014. "Big Data Surveillance: Introduction." *Surveillance & Society* 12(2): 185-196.

Agamben, Giorgio. *State of Exception*. Chicago: Chicago University Press.

Attride-Stirling, Jennifer. 2001. "Thematic networks: an analytical tool for qualitative research." *Qualitative Research* 1(3): 385-405.

Audit Commission. 1993. *Helping with Enquiries: Tackling Crime Effectively*. Audit Commission, London.

Bayley, David. 1998. *What Works in Policing.* Oxford University Press: New York.

Bayley, David and Clifford Shearing. 2001. *The New Structure of Policing: Description, Conceptualization, and Research Agenda*. U.S. Department of Justice: National Institute of Justice.

Baxter, Pamela and Susan Jack. 2008. "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers." *The Qualitative Report* 13(4): 544-559.

Beardwood, John. 2003. "Creeping law? An analysis of the Canadian Lawful Access Consultation Document and its approach to implement the Council of Europe's convention on cyber-crime." *Computer Law Review International* 3: 77-83.

Beck, Ulrich. 2002. "The Terrorist Threat: World Risk Society Revisited." *Theory, Culture & Society* 19(4): 39-55.

Beck, Ulrich. 2009. "Critical Theory of World Risk Society: A Cosmopolitan Vision." *Constellations* 16(1): 3-22.

Bendrath, Ralf. 2001. "The Cyberwar Debate: Perception and Politics is US Critical Infrastructure Protection". *Information & Security* 7: 80-103.

Bennett, Colin., Haggerty, Kevin., Lyon, David and Valerie Steeves. 2014 (Eds). *Transparent Lives: Surveillance in Canada*. Athabasca University Press: Edmonton.

Bennett, Colin. 2001. "Cookies, web bugs, webcams and cue cats: patterns of surveillance on the world wide web." *Ethics and Information Technology* 3(3): 195-208.

Berry, David. 2012. "The Social Epistemologies of Software." *Social Epistemology* 26(3-4): 379-398.

Brodeur, Jean-Paul. 2007. "High and Low Policing in Post-9/11 Times." *Policing* 1(1):25-37.

Brodeur, Jean-Paul and Benoit Dupont. "Knowledge Workers or 'Knowledge' Workers?" *Policing & Society* 16(1): 7-26.

Bronskill, Jim. 2014. "Spy agency uncovers 'serious breaches'". *Metro News, Canada, http://metronews.ca/news/canada/973382/spy-agency-uncovers-serious-breaches/* (accessed on April 20, 2015).

Brennan, Julia. 2005. "Mixed Methods: The Entry of Qualitative and Quantitative Approaches in the Research Process." *International Journal of Social Research Methodology,* Vol 8(3):173-184.

Button, Mark. 2012. *Private Policing*. UK: Willan Publishing.
Burton, Frank and Pat Carlen. 1979. *Official Discourse: On Discourse Analysis, Government Publications, Ideology and the State*. London: Routledge and Kegan Paul.
Castells, Manuel. 1996. *The Rise of the Network Society: The Information Age: Economy, Society and Culture (Vol. 1)*. Massachusetts and Oxford: Blackwell.
Casey, Sean. 2013. "[Lawful Access]". In Canada. Parliament. House of Commons. *Debates*. 41st Parliament, 2nd Session, Vol. 147 (November 27, 2013). Ottawa: Canadian Government Publishing: 1421-1463.
Canadian Privacy Commissioner 2014. Metadata and Privacy: A Technical and Legal Overview."
Carter, David. 2004. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. Michigan State University and US Department of Justice Office of Community Oriented Policing Services.
Carter, David and Jeremy Carter. 2009. "Intelligence Led Policing: Conceptual and Functional Considerations for Public Policy." *Criminal Justice Policy Review* 20(3): 310-325.
Callon, Michel. 1986. "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen. Power, Action and Belief: A New Sociology of Knowledge." Pp. 57-78 in *Technoscience: The Politics of Interventions,* edited by Asdal, Kristin, Brita Brenna, and Ingunn Moser, 2007. Oslo Academic Press.
CBC News. August 25, 2015. "Nova Scotia anti-cyberbullying law challenged in Supreme Court".
Coleman, Gabriella. 2013. "Anonymous in Context: The Politics and Power behind the Mask." *Centre for International Governance Innovation* 3:1-21.
Conway, Maura. 2007. "Cyberterrorism: Hype and reality." In *Information Warfare* by E.L. Armistead (ed). Virginia: Potomac Books.
Convention on Cybercrime. 2001.
Cyber-Security Stategy 2010 by GoC.
Clarke, Richard and Robert Kanake. 2010. *Cyber war: the next threat to national security and what to do about it*. New York: HarperCollins.
Clarke, Roger. 1998. "Information Privacy on the Internet: Cyberspace Invades Personal Space." *Telecommunication Journal of Australia* 48(2): 61-67.
Charmaz, Kathy. 2006. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. California: SAGE.
Crawford, Adam. 2006. "Networked Governance and the Post-Regulatory State? Steering, Rowing and Anchoring the Provision of Policing and Security." *Theoretical Criminology* 10(4): 449–79.
De Lint, Willem. 2006. "Intelligence in Policing and Security: Reflections on Scholarship." *Policing and Society* 16(1): 1-6.
Deukmedjian, John., and Willem de Lint. 2007. "Community into Intelligence: Resolving Information uptake in the RCMP." *Policing & Society* 17(3): 239-256.
Deibert, Ronald. 2013. *Black Code: Inside the Battle for Cyberspace*. Oxford: Signal.
Denning, Dorothy. 2000. *Testimony before the Special Oversight Panel on Terrorism*. Committee on Armed Services: U.S. House of Representatives.
Denning, Dorothy. 2001. "Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy". *Rand Monograph Report*s.

Denning, Dorothy. 2012. “Stuxnet: What Has Changed?” *Future Internet* 4:672-687.
Duhigg, Charles. 2012. “How Companies Learn Your Secrets”. http://128.59.177.251/twiki/pub/CompPrivConst/HowCompaniesLearnOurConsumingSecrets/How_Companies_Learn_Your_Secrets_-_NYTimes.com.pdf
Dupont, Benoit. 2008. “Hacking the Panopticon: Distributed Online Surveillance and Resistance” in *Surveillance and Governance: Crime Control and Beyond (Sociology of Crime, Law and Deviance) Vol. 10* by Mattieu Deflem (Eds). Oxford: Elsevier.
Escudero-Pascual, Alberto and Ian Hosein. 2004. “Questioning lawful access to traffic data.” *Communications of the ACM* 47(3): 77-82.
Ericson, Richard and Kevin Haggerty. 1997. *Policing the Risk Society*. Oxford University Press: United Kingdom.
Fagan, Jeffrey and Garth Davies. 2000. “Street Stops and Broken Windows: Terry, Race and Disorder in New York City.” *Fordham Urban Law Journal* 28: 457-504.
Farrington, David, and Donald West. 1993. “Criminal, Penal and Life Histories of Chronic Offenders: Risk and Protective Factors and Early Identification.” *Criminal Behaviour and Mental Health* 3: 492-523.
Fairclough, Norman. 1989. *Language and Power*. London: Routledge.
---------. 1995. *Critical Discourse Analysis: The Critical Study of Language*. London: Routledge.
---------. 2003. *Analysis discourse: Textual analysis for social research*. Younganthropologist.com
Forcese, Craig. 2007. *Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the use of ‘Special Advocates’ in National Security Proceedings*. Study commissioned by the Canadian Centre for Intelligence and Security Studies. Ottawa: University of Ottawa.
Forcese, Craig and Kent Roach. 2015. *False Security: The Radicalization of Canadian Anti-Terrorism*. Toronto: Irwin Law Books.
Frost & Sullivan. 2011. “Lawful Interception: A Mounting Challenge for Service Providers and Governments.” *Frost & Sullivan.*
Francis, Hannah. 2015. “Metadata spying by local councils on the rise.” *Sydney Herald, Tech, http://www.smh.com.au/technology/technology-news/metadata-spying-by-local-councils-on-the-rise-20150619-ghs0dg.html* (access on March 10, 2015).
Flyvbjerg, Bent. 2001. *Making Social Science Matter: Why social inquiry fails and how it can succeed again*. New York: Cambridge University Press.
Foucault, Michel. 1991. *Discipline and Punish: The Birth of the Prison*. UK: Penguin.
Fuchs, Christian. 2012. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. United Kingdom: Routledge.
Gallagher, Ryan. 2014. “The Surveillance Engine: How the NSA Built Its Own Secret Google”. https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/ (accessed May 01, 2015).
Gallahger, Ryan and Glenn Greenwald. 2015. “Canadian Spies Collect Domestic Emails in Secret Security Sweep”. https://firstlook.org/theintercept/2015/02/25/canada-cse-pony-express-email-surveillance/ (accessed May 01, 2015).
Garland, David. 2001. *The Culture of Control: Crime and Social Order in Contemporary Society*. USA: Oxford University Press.

Geertz, Clifford. 1973. “Thick description: Toward an interpretive theory of culture.” Pp. 3-30 in *The Interpretation of Cultures: Selected Essays*. New York: Basic Books.
Gentile, Patricia. 2009. “Resisted access? National security, the Access to Information Act, and queer(ing) archives.” *Archivaria* 68: 141-158.
Geist, Michael. [Legal and Constitutional Affairs Debates]. In Canada. Parliament. Proceedings of the Standing Senate Committee. *Debates*. 41st Parliament, 2nd Session, No. 21 (November 20, 2014). Ottawa: Canadian Government Publishing.
Guidetti, Ray and Thomas Martinelli. 2009. “Intelligence-led policing: A Strategic Framework.” *Police Chief* 76(10): 132, 134, 136.
Gill, Peter. 2006. “Not Just Joining the Dots But Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2001.” *Police and Society* 16(1): 27-49.
Gillis, A.R. 1989. “Crime and State Surveillance in Nineteenth-Century France.” *American Journal of Sociology* 95(2): 307-341.
Gallagher, Ryan. 2015. “Documents Reveal Canada’s Secret Hacking Tactics”. *The Intercept*: https://firstlook.org/theintercept/2015/03/23/canada-cse-hacking-cyberwar-secret-arsenal (accessed on March 29, 2015).
Gignac, Tamara. 2013. “‘Cyber version of Pearl Habor’ looms over energy industry; security expert warns Canada at risk’.” *Calgary Herald, News,* February 25,2013.
Galloway, Alexander R. 2004. *Protocol: How Control Exists After Decentralization*. MIT Press.
Greenberg, Joshua. 2000. “Opinion Discourse and Canadian Newspapers: The Case of the Chinese Boat People.” *Canadian Journal of Communication* 25:517-534.
Greenwald, Glenn. 2014. *No Place to Hide*: *Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.
Gendron, Angela. 2013. “Cyber threats and multiplier effects: Canada at risk.” *Canadian Foreign Policy Journal* 19(2):178-198.
Greene, Jennifer., Caracelli, Valeries and Wendy Graham. “Toward a Conceptual Framework for Mixed-Method Evaluation Designs.” *Education, Evaluation and Policy Analysis* 11(3): 255-274.
Gergen, Kenneth. 1999. *An Invitation to Social Construction*. California: SAGE.
Goffman, Erving. 1959. *The Presentation of Self in Everyday Life*. New York: Anchor Books.
Haggerty, Kevin and Richard Ericson. 2000. “The surveillant assemblage.” *British Journal of Sociology* 51(4): 605-622.
Hafner, Katie and Matthew Lyon. 1996. *Where the wizards stay up late: the origins of the Internet*. Simon & Schuster: New York.
Hesse-Biber, Sharlene Nagy, and Patricia Leavy. 2011. *The Practice of Qualitative Research* (ed. 2). New York: SAGE publications.
Huey, Laura and Richard Rosenberg. 2006. “Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention.” *Canadian Journal of Criminology and Criminal Justice* 46(5): 597-606.
Hua, Jian and Sanjay Bapna. 2012. “The economic impact of cyber terrorism.” *Journal of Strategic Information Systems.*

Hough, Mike and Pat Mayhew. 1985. “Taking Account of Crime: Key Finding From the Second British Crime Survey.” *Home Office Research Study No. 85*. London: Her Majesty’s Stationary Office.
Janks, Hilary. 1997. “Critical Discourse Analysis as a Research Tool.” *Discourse: studies in the cultural politics of education* 18(3): 329–42.
Jenion, Greg. “Beyond ‘what works’ in reducing crime: the development of a municipal community safety strategy in British Columbia”.
Johnson, Jim. 1988. “Mixing Humans and Nonhumans Together: The Sociology of a Door-Closer.” *Social Problems* 35(3): 298–310.
Joh, Elizabeth. 2014. “Policing by Numbers: Big Data and the Fourth Amendment.” *Washington Law Review*.
Jones, Trevor and Tim Newburn. 1998. *Private Security and Public Policing*. NY: Oxford University Press.
Jones, Trevor and Tim Newburn. 2006. *Plural Policing: A Comparative Perspective*. UK: Routledge.
Jørgensen, Marianne, and Louise Phillips. 2002. *Discourse Analysis: as Theory and Method*. London: SAGE Publications.
Kelling, George L., and William J. Bratton. 2006. “Policing Terrorism.” *Civic Bulletin* 43(9): 1-6.
Larsen, Mike. 2013. *Access in the Academy: Bringing ATI and FOI to academic research.* Vancouver: British Columbia Freedom of Information and Privacy Association.
Larsen, Mike and Kevin Walby (Eds). 2012. 2012. *Brokering Access: Power, Politics, and Freedom of Information Process in Canada*. Vancouver: UBC Press.
Law, John. 2009. “Actor Network Theory and Material Semiotics.” Pp. 141-158 in *The New Blackwell Companion to Social Theory* by Brian Turner (Eds). Blackwell Publishing: UK.
Latour, Bruno. 1987. *How to Follow Scientists and Engineers through Society*. Massachusetts: MIT Press.
Latour, Bruno. 2005. *Reassembling the Social: An Introduction to Actor-Network Theory*. New York: Oxford University Press.
Laclau, Ernesto, and Chantal Mouffe. 1985. *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics*. London: Verso.
Lewis, James. 2003. “Cyber Terror: Missing in Action.” *Knowledge, Technology, and Society* 16(2):34-41.
Levin, Avner and Paul Goodrick. 2013. “From cybercrime to cyberwar? The international policy shift and its implications for Canada?” *Canadian Foreign Policy Journal* 19(2):127-143.
Leblanc, Daniel. 2009. “Harper to shut down Parliament”. *CBC News, Politics,* http://www.theglobeandmail.com/news/politics/harper-to-shut-down-parliament/article4300862/ (accessed on March 29, 2015).
Lyon, David. 2003. *Surveillance After September 11*. Cambridge: Polity.
Lyon, David. 2014. “Surveillance, Snowden, and Big Data: Capacities, consequences, critque.” *Big Data & Society*: 1-13.
Loughlin, Matt. 2011. “Is the Gestapo Everywhere? The Origins of the Modern Perception of the Secret Police of the Third Reich.” *Legacy* 11(1): 51-58.

Marcon, Alessandro. 2015. *The Discursive Enactment of Edward Snowden*. Master's thesis. Carleton University.
Marwick, Alice E. "The Public Domain: Social Surveillance in Everyday Life." *Surveillance & Society* 9(4): 378-393.
Mann, Bruce. 2009. "Lawful Trojan Horse." *Forthcoming.*
Malone, Eloise and Michael Malone. 2013. "The 'Wicked Problems' of cybersecurity policy: analysis of United States and Canadian policy response." *Canadian Foreign Policy Journal* 19(2): 158-177.
Maurushat, Alana. 2012. "Ethical Hacking: A Report for A Report for the National Cyber Security Division of Public Safety Canada".
Maurushat, Alana. 2013. "From cybercrime to cyberwar: security through obscurity or security through absurdity?" *Canadian Foreign Policy Journal* 19(2):119-122.
Maguire, Mike. 2000. "Policing by risks and targets: some dimensions and implications of intelligence-led crime control." *Policing and Society* 9(4):315-336.
Maguire, Mike, and Tim John. 2006. "Intelligence Led Policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK." *Police and Society* 16(1): 67-85.
Mayer-Schoenberger, Viktor and Kenneth Cukier. 2013. *Big Data: A Revolution that will transform how we live, work, and think*. London: John Murray Publishers.
MacKay, Peter. [House Debates]. In Canada. Parliament. House of Commons. *Debates*. 41st Parliament, 2nd Session, Vol. 147, No. 25 (November 27, 2013). Ottawa: Canadian Government Publishing.
MacKay, Peter. [House Debates]. In Canada. Parliament. House of Commons. *Debates*. 41st Parliament, 2nd Session, Vol. 147, No. 120 (October 1, 2014). Ottawa: Canadian Government Publishing.
McGarrell, Edmund, Joshua Freilich, and Steven Chermak. 2007. "Intelligence-Led Policing As a Framework for Responding to Terrorism." *Journal of Contemporary Criminal Justice* 23: 142-158.
Mills, C. Wright. 1956. *The Power Elite*. USA: Oxford University Press.
Moffitt, Terrie. 1993. "Adolescence-limited and Life-course-persistent Antisocial Behavior: a Developmental Taxonomy." *Psychological review* 100(4):674-701.
Murphy, Christopher. 2007. "'Securitizing' Canadian Policing: A New Policing Paradigm For the Post 9/11 Security State?" *Canadian Journal of Sociology* 32(4): 449-475.
Monaghan, Jeffrey. 2014. "Security Traps and Discourses of Radicalization: Examining Surveillance Practices Targeting Muslims in Canada." *Surveillance & Policing* 12(4): 485-501.
Mol, Annemarie. 2010. "Actor-Network Theory: Sensitive Terms and Enduring Tensions." *Kölner Zeitschrift für Soziologie und Sozialpsychologie. Sonderheft* 50:253–69.
Mopas, Michael. 2009. *Imagining the Internet and making it governable: Canadian law and regulation*. Phd Dissertation. University of Toronto.
Olson, Parmy. 2012. *We are anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency*. Hachette Digital, Inc.
Oxblood Ruffin. 2004. "Hacktivism, from here to there." *Cult of the Dead Cow.*

Parsons, Christopher. 2012. “Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm, and Future Canadian Policies.” *Draft Version 2.2.*
Parsons, Christopher. 2015. “Do Transparency Reports Matter for Public Policy? Evaluating the effectiveness of telecommunication transparency reports.” *Draft Version 1.4.*
Pardy, Carson. [Standing Committee on Justice and Human Rights Debates]. In Canada. Parliament. House of Commons Committee Debates. *Debates*. 41st Parliament, 2nd Session, No. 25 (May 15, 2014). Ottawa: Canadian Government Publishing.
Payton, Laura. 2013. “Government killing online surveillance bill.” *CBC News, Politics, http://www.cbc.ca/news/politics/government-killing-online-surveillance-bill-1.1336384* (accessed on March 29, 2015).
Pilieci, Vito. 2010. “Canada unprepared or massive attack: expert.” *Ottawa Citizen,* March 23, 2010.
Piche, Justin. 2012. “Accessing the State of Imprisonment in Canada: Information Barriers and Negotiation Strategies.” Pp. 234-260 in *Brokering Access: Power, Politics, and Freedom of Information Process in Canada* by Mike Larsen and Kevin Walby (eds). Canada: UBC Press.
Pugliese, David. 2000. “Blame Canada for 80% of cyber-attacks: Country a ‘zone of vulnerability,’ U.S. Military Report Warns.” *Ottawa Citizen,* March 20, 2000.
Primoratz, Igor. 1990. “What is Terrorism?” *Journal of Applied Philosophy* 7(2): 129-138.
Public Safety Canada. 2014. “Cyber Security: A Shared Responsibility.” *Government of Canada.* http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-eng.aspx
Priest, Dana. 2013. “NSA growth fueled by need to target terrorists.” http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html
Ratcliffe, Jerry, and Ray Guidetti. 2008. “State police investigative structure and the adoption of intelligence-led policing.” *An International Journal of Police Strategies and Management 31(1): 109-128.*
Ratcliffe, Jerry. 2002. “Intelligence-led Policing and the Problems of Turning Rhetoric into Practice.” *Policing & Society* 12(1): 53–66.
---------. 2003. “Intelligence-led policing.” *Trends and Issues in Crime and Criminal Justice* 248:1-6.
---------. 2012. *Intelligence-led Policing*. Abingdon: Routledge.
Reinharz, Shulamit. 1992. *Feminist methods in social research*. Oxford: Oxford University Press.
Roberts, Alasdair. 2002. “Administrative Discretion and the Access to Information Act: An ‘internal Law’ on Open Government?” *Canadian Public Administration* 45(2): 175–194.
Roe, Brent and Jeannie Bail. 2012. “Lawful Access Legislation, Its Risks and Why Libraries Must Care.” *World Library and Information Congress—78th IFLA General Conference and Assembly,* Session: 166 — Master of contents or How to win the battle over freedom in cyberspace? — Free Access to Information and Freedom of Expression (FAIFE) with Copyright and other Legal Matters (CLM).

Rosenbaum, Denis. 1987. “The Theory and Research Behind Neighborhood Watch: Is It a Sound Fear and Crime Reduction Strategy?” *Crime & Delinquency* 33(1): 103-134.
Rallis, Sharon and Gretchen Rossman. 2010. *The Research Journey: Introduction to Inquiry*. New York: Guildford Press.
Rudner, Martin and Angela Gendron. 2013. “Assessing Cyber Threats.” A Report Prepared for the Canadian Security Intelligence Service.
Royal Canadian Mounted Police. 2014. “Cybercrime: An Overview of Incidents and Issues in Canada”. *Her Majesty the Queen in Right of Canada*.
Raboy and Shtern 2010.
Shade, Leslie. 2008. “Reconsidering the Right to Privacy in Canada.” *Bulletin of Science Technology Society* 28(1): 80-91.
Sherman, Lawrence. 1986. “Policing Communities: What Works?” *Crime and Justice* 8: 343-386.
Singer, Peter. 2014. “Squirrels: A Bigger Threat than Cyber Terrorists?” *Cybersecurity:* Brookings Institute. http://www.brookings.edu/blogs/brookings-now/posts/2014/01/squirrels-a-bigger-threat-than-cyber-terrorists
Schneier, Bruce. 2014. *Data and Goliath*: *The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company: New York, USA.
Schneier, Bruce. 2015. Metadata = Surveillance”. https://www.schneier.com/essays/archives/2014/03/metadata_surveillanc.html
https://www.schneier.com/blog/archives/2014/03/metadata_survei.html
Schmitt, Carl. 2005. *Political Theology: Four Chapters on the Concept of Sovereignty*. Translated by G. Schwab. Chicago: University of Chicago Press.
Sheptycki, James. 2004. “Organizational Pathologies in Police Intelligence Systems: Some Contributions to the Lexicon of Intelligence-Led Policing.” *European Journal of Criminology* 1(3): 307-332.
Shearing, Clifford and Philip Stenning. 1987. “Reframing policing” in *Private Policing* by Clifford Shearing and Stenning (eds). California: SAGE.
Spratt, Michael. [Standing Committee on Justice and Human Rights Debates]. In Canada. Parliament. House of Commons Committee Debates. *Debates*. 41st Parliament, 2nd Session, No. 26 (May 27, 2014). Ottawa: Canadian Government Publishing.
Stohl, Michael. 2006. “Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games?” *Crime, Law, and Social Change* 46:223-238.
Strauss, Anselm and Juliet Corbin. 1990. *Basics of qualitative research: Grounded theory procedures and techniques*. Thousand Oaks, CA: Sage Publications.
Soghoian, Christopher. 2012. *The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance*. PhD Dissertation: Indiana University.
Swire, Peter. 2012. “From real-time intercepts to stored records: why encryption drives the government to seek access to the cloud.” *International Data Privacy Law* 2(4): 200-206.
Singer, Peter W and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.
Skogan, Wesley. 1977. “Dimensions of the Dark Figure of Unreported Crime. *Crime & Delinquency,* 43: 41-50.

Statistics Canada. 2002. “Cyber-crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics.” *Canadian Police College*. Catologue No. 85-558-XIE.
Statistics Canada. 2009. “Private security and public policy.” *http://www.statcan.gc.ca/pub/85-002-x/2008010/article/10730-eng.htm*
Statistics Canada. 2013. “Police-reported crime statistics in Canada, 2012.” http://www.statcan.gc.ca/pub/85-002-x/2013001/article/11854-eng.htm
Statistics Canada. 2014a. “Uniform Crime Report.” http://www23.statcan.gc.ca/imdb/p2SV.pl?Function=getSurvey&SDDS=3302
Statistics Canada. 2014b. “Police-reported cybercrime in Canada, 2012.” http://www.statcan.gc.ca/daily-quotidien/140925/dq140925b-eng.htm?HPA
Statistics Canada. 2015. “Uniform Crime Reporting Survey (UCR).” http://www23.statcan.gc.ca/imdb/p2SV.pl?Function=getSurvey&SDDS=3302
Tenorio, Encarnacion Hidalgo. “Critical Discourse Analysis, An overview.” *Nordic Journal of English Studies* 10(1): 183-210.
Therrien, Daniel. 2015. “Submission to the Standing Committee on Industry, Science and Technology.” *Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act (the Digital Privacy Act*).
Thorsen, Dag and Amund Lie. 2006. “What is Neoliberalism?” http://folk.uio.no/daget/What%20is%20Neo-Liberalism%20FINAL.pdf
Trottier, Daniel. 2012. “Policing social media.” *Canadian Review of Sociology* 49(4): 411-425.
Toews, Vic, [House Debates]. In Canada. Parliament. House of Commons. *Debates*. 41st Parliament, 2nd Session, Vol. 146 (February 13, 2012). Ottawa: Canadian Government Publishing: 5163-5231.
Tsoukala, Anastassia. 2008. “Boundary-creating Processes and the Social Construction of Threat.” *Alternatives: Global, Local, Political* 33(2): 137-152.
Tufekci, Zeynep. 2014. “Engineering the public: Big data, surveillance and computational politics.” *First Monday* 19(7).
Valiquet, Dominique. 2011. “Cybercrime: issues”. *Library of Parliament*, Background Paper No. 2011-36.
Van Dijck, Jose. 2014. “Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology.” *Surveillance & Society* 12(2): 197-208.
Van Otterlo, Martijn. 2014. “Automated experimentation in Walden 3.0: The next step in profiling, predicting, control and surveillance.” *Surveillance & Society* 12(2): 255-272.
Wallace, Mike. [House Debates]. In Canada. Parliament. House of Commons. *Debates*. 41st Parliament, 2nd Session, Vol. 147, No. 120 (October 1, 2014). Ottawa: Canadian Government Publishing.
Wall, David and Matthew Williams. "Policing diversity in the digital age Maintaining order in virtual communities." *Criminology and Criminal Justice* 7(4): 391-415.
Walby, Kevin and Mike Larsen. 2012. “Access to Information and Freedom of Information Requests: Neglected Means of Data Production in the Social Science.” *Qualitative Inquiry* (18)1: 31-42.

Walby, Kevin and Mike Larsen. 2012. *Brokering Access: Power, Politics, and Freedom of Information Process in Canada,* edited by Mike Larsen and Kevin Walby. Vancouver: UBC Press.

Wellman, Barry. 2001. "Physical place and cyberplace: The rise of personalized networking." *International journal of urban and regional research* 25(2): 227-252.

Weimann, Gabriel. 2004. “Cyberterrorism: How Real is the Threat?” *United States Institute of Peace: Special Report* 119.

Weimann, Gabriel. 2008. “Al Quaida’s Extensive Use of the Internet”. *CTC Centenial* 1(2): 607.

Wilks, David. [House Debates]. In Canada. Parliament. House of Commons. *Debates*. 41st Parliament, 2nd Session, Vol. 147, No. 75 (April 28, 2014). Ottawa: Canadian Government Publishing.

Weber, Amalie. 2003. “The Council of Europe’s Convention on Cybercrime.” *Berkeley Technology Law Journal* 18(1):425-446.

Whitaker, Reg. “The Curious Tale of the Dog That Hasn’t Barked (Yet).” *Surveillance & Society* 10(3/4): 340-343.

Young, Jason. 2004. “Surfing while Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation—A Critical Analysis of the Council of Europe Convetion on Cybercrime and the Canadian Lawful Access Proposal.” *7 Yale J.L. & Tech. 346, 374.*