

**DANGEROUS TECHNOLOGIES AND THE LOSS OF PRIVACY RIGHTS:
ANALYZING CANADIAN LAWFUL ACCESS LEGISLATION THROUGH SOCIAL
PROBLEM THEORY**

BRENT NELLIS

Thesis submitted to the University of Ottawa
in partial Fulfillment of the requirements for the
Doctorate in Philosophy degree in Criminology

Department of Criminology
Faculty of Social Sciences
University of Ottawa

Table of Contents

Table of Contents	ii
Abstract	v
Introduction	1
Criminological Interests	3
Canadian Lawful Access Legislation	12
Thesis Outline	17
Chapter 1: Risk and the Expansion of Canadian Surveillance	19
Surveillance and the Canadian Identity	25
The Extension of Surveillance in Space and Time	30
Democratic Implications of Opacity and Transparency	36
Conclusion	40
Chapter 2: Theoretical Framework and Methodology	43
Epistemological Foundation	45
Weak Readings of Social Problem Theory	55
Weak Readings Based on the Integration of Subjective and Objective Social Conditions ...	55
Weak Readings Based on Critiques	58
Contextual Constructionism	60
Reconciling a Strong Reading with Contextual Constructionism	61
The Components of Claims	62
Condition-Categories	65
Rhetorical Idioms	67
Rhetorical Motifs	69
Counter-rhetorics	70
Claims-making Styles	72
Research Methods	73
Data Collection	73
Coding	75
Conclusion	83
Chapter 3: Endangerment from New Technologies	85
Grounds	87
Old Crimes and New Technologies	88

New Crimes for New Technologies.....	91
Cyberbullying.....	92
Common Grounds.....	99
Domain and Orientation	101
Warrants.....	106
Protection Based on Obligation.....	107
Protection of Vulnerable Children.....	110
Protection as a Response to the Fear of Crime.....	112
The Conclusions of the Claim.....	118
Chapter 4: Loss of Privacy, Part 1	128
Grounds.....	130
Privacy and Democratic Civil Rights	130
Privacy and Oversight	142
Privacy and Political Partisanship	147
Domain and Orientation	160
Reviewing the Grounds of the Loss of Privacy.....	162
Warrants.....	163
The Balance of Security and Privacy	164
Democratic Civil Rights	167
The Conclusions of the Claim.....	169
Chapter 5: Loss of Privacy, Part 2	173
Grounds.....	176
The Trivialization of Personal Information and Surveillance	176
Oversight Measures	180
Normalization of New Surveillance by the Old	185
Domain and Orientation	190
Warrants of Obligation and Balance	191
Conclusions of the Claim	194
Chapter 6: Discussion	200
Constructing (In)Security.....	202
Defining Privacy	206
Reconceptualizing Privacy Rights	210

The Natural History Model	220
Conclusion	222
References	226

Abstract

This project analyzes efforts to “modernize” Canadian lawful access legislation, focusing primarily on legislation proposed by the Conservative government between 2009 and 2014. Though privacy is a democratic right integral to citizens’ political participation, research shows that governments often mobilize security threats to justify the expansion of surveillance measures that infringe upon privacy rights, citing the need to “balance” national security and civil rights. The purpose of this project is to understand how security and privacy were socially constructed in relation to lawful access legislation. Using social problem theory, which studies how social problems are socially constructed through the rhetorical claims-making activities of relevant parties, this project examines newspaper articles, parliamentary records, and government documents to understand how political parties, lawyers, privacy advocates, victims’ advocates, and other claims-makers defined the security and privacy issues that surrounded lawful access legislation. Similarly to broader trends, the endangerment of Canadian society by cybercrime and cyberbullying and the loss of privacy rights were prominent issues in the rhetoric, as was the need to balance security and privacy. However, the analysis shows that proponents of lawful access legislation took a nuanced approach to the balance between security and privacy by claiming that the legislation would respect and protect privacy rights. This rhetorical claim subverted the common framing of security and privacy as mutually exclusive benefits in a zero-sum game. This suggests that defending privacy rights on the grounds that they are equal to security rights would be an ineffective strategy, as the state can simply deny claims that its policies would infringe upon privacy rights.

Introduction

This research project examines the rhetorical discourse that surrounded Canadian lawful access legislation between 2009 and 2014.¹ During this period, the Canadian government, including governments formed by two different parties, attempted to implement laws meant to “modernize” lawful access of data and communications through surveillance and interception in order to adapt state and police practices to developing telecommunication technologies and networked technologies. Canadian privacy rights had been heavily influenced by section 8 of the *Canadian Charter of Rights and Freedoms*, which guarantees protection from unlawful search and seizure (Bailey, 2008; Canadian Charter of Rights and Freedoms, 1982, s 8). However, as technology was evolving, the practical and legal realities of “search” and “seizure” had become increasingly complex.

Certainly, the development of networked technologies has significantly changed how information, including intimate personal information, is used, shared, stored, published, accessed, and intercepted. Deleuze (1995) describes the modern era in terms of “control societies that no longer operate by confining people but through continuous control and instant communication” (p. 174), a system of social institutions built on the premise that “[t]he digital language of control is made up of codes indicating whether access to some information should be allowed or denied” (p. 180). Access to and movement through social institutions is regulated by these codes. Indeed, Lyon (2003) argues that while mechanisms of classifications themselves are not new, “classification processes are being automated and used for a variety of tasks within

¹ This project includes data outside this time period, either to provide additional context or because it was initially included in the data collection. However, the legislation proposed between 2009 and 2014 became the focus of this research because it represented continuous attempts to “modernize” lawful access legislation by the then-Conservative government of Canada.

increasingly dominant forms of risk management” (p. 150), which increasingly subjects citizens to the control society’s surveillance infrastructure. Showing the extensive reach of modern technologies in citizens’ daily lives, a report by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada (2013) stats that an internet protocol (IP) address, identifying information that is necessary to most if not all internet-based activities, can provide information about the ownership of servers, the physical location of a computer, and the e-mail addresses used by a particular IP address, all of which can be used to obtain more information about an individual’s identity, and miscellaneous internet activities such as file-sharing or web activities and posts that could in turn reveal information about the user’s personal beliefs and habits. Evidently, the technologies used to access the internet can also be used to expose deeply intimate details about someone’s personal life.

From this perspective, surveillance is an important issue for criminological inquiry. As Lessig (1999a) explains, surveillance relies on real-time monitoring or searching information after the fact in order to observe its subject, so the ease and efficiency of monitoring and searching heavily influences surveillance capabilities. In the past, this type of surveillance required significant resources, as the physical presence of police and government agents was the only way to monitor subjects and record information about their activities. Modern digital technologies, however, have made surveillance much easier and more efficient, especially within the context of the control society and its constant tracking and recording of personal information as individuals move between social institutions.

As part of the digital monitoring process, information is recorded so that it can be referenced – searched – later if needed, and brief moments in time become semi-permanent. Moreover, because the surveillance process is built into the technology as a fundamental,

necessary feature, direct, real-time monitoring is no longer the only – or even the preferable – option, as “[m]ore can be searched, as more data are collected [and] searching is cheaper, as the monitored becomes more easy to scan” (Lessig, 1999a, p. 60). Because personal information is now so easily shared and accessed, “changing technologies reduce the legal justifications for interfering with the searches” (Lessig, 1999a, p. 61). Individuals willingly share their personal information with others, with corporations and service providers, with the government, and with technological infrastructure in order to participate in society. As a result, Lessig (1999a) argues, legal privacy has been depreciated, raising important and pressing questions about the surveillance mechanisms integrated into networked technologies and their impact on the search and seizure laws which have traditionally restricted state power.

Furthermore, Lessig’s (1999b) analysis of cyberspace brings attention to coordinating standards – “a rule that facilitates an activity that otherwise would not exist” (p. 759) – and regulating standards – which “restricts behavior within that activity, according to a policy set by the regulators” (p. 759) – and warns that governments will “regulate by regulating the *code* that regulates the behavior of people in cyberspace” (p. 763, emphasis in original). Thus, integrating monitoring and searching in the code of cyberspace would allow the state to regulate citizens’ online behaviours by forcing citizens to interact with surveillance mechanisms in order to access cyberspace at all. This would exacerbate the depreciation of privacy and pose a risk to the political agency and autonomy of citizens, who would be placed under the constant – albeit indirect – influence of the state.

Criminological Interests

This depreciation of privacy is a subject of criminological interest because surveillance is a key component of policing and, by extension, of state control and state violence. Justice Gerard

La Forest emphasizes the importance of privacy protections, especially privacy from the state, in several court cases related to s. 8 of the *Charter of Rights and Freedoms* (1982) which guarantees the right of individuals to be free from unreasonable search and seizure. In addition to the *Charter*, the *Privacy Act* (1985) set standards for how government agencies could and should use personal data, while the *Personal Information Protection and Electronic Documents Act* (PIPEDA) (2000) regulates the use of personal information by private companies, precisely to protect individuals from undue interference.

For example, in *Dyment*, La Forest posits that privacy is integral to “physical and moral autonomy” (*R. v. Dyment*, 1988, para. 17) and is “essential for the well-being of the individual” (*R. v. Dyment*, 1988, para. 17) because “it is for the individual to determine the manner in which he or she will order his or her private life” (*Thomson Newspapers Ltd. v. Canada*, 1990, p. 517).

Physical monitoring forces individuals to account for their movements and activities and moral monitoring forces individuals to account for their personal beliefs and inclinations. Furthermore, information obtained through surveillance can lead to further investigation (*R. v. Evans*, 1996), increasing the risk that the subject of surveillance will be criminalized, and investigations can affect a suspect’s reputation negatively regardless of their outcome (*Thomson Newspapers Ltd. v. Canada*, 1990). In these conditions, individuals would potentially feel compelled to constantly justify themselves and possibly expose more intimate details of their personal lives in order to do so, which would greatly constrain their personal freedom to act in society.

There is historical evidence to support La Forest’s perspective. Canadian colonialism made extensive use of surveillance to police First Nations and Indigenous peoples (Crosby and Monaghan, 2016; Howe and Monaghan, 2016; Proulx, 2014), police spied on "Communist" labour organizations that were active during the first half of the 20th century (Axelrod, 1995;

Kealey, 1992; Lonardo, 1995; Parnaby and Kealy, 1997), the federal government of the 1950s and 1960s used surveillance to identify gay and lesbian employees of the civil service so they could be purged because they were considered potential targets for blackmail by foreign countries (Kinsman, 1995). More recently, surveillance has once again been implicated in security measures implemented after the 9/11 terrorist attacks which commonly perpetuated islamophobia and anti-Muslim discrimination (Jamil, 2017; Nagra and Maurutto, 2016). Because of government surveillance and monitoring, the individuals involved were denied the freedom to order their lives according to their cultural traditions, political beliefs, sexual orientation, or religious beliefs.

If privacy is therefore a necessary condition of personal autonomy, as LaForest suggests, then it is important to closely evaluate the reasons behind any legislation that weakens s.8 as it is “intended to afford protection to all of us to be secure against intrusion by the state or its agents by unreasonable searches or seizures, and is not solely for the protection of criminals even though the most effective remedy will inevitably protect the criminal as the price of liberty for all” (*R. v Edwards*, 1996, para. 59). Without privacy, freedom shrinks and all individuals, but especially the most marginalized, are opened up to greater control by the state.

Early common law jurisprudence linked restrictions on police search and seizure to the right to enjoy property and trespass laws (*Hunter et al. v. Southam Inc.*, 1984). This was seen as especially important because “[a]ttempts by police to enforce the law at people's dwellings frequently leads to confrontations that can have far more serious consequences than the evil sought to be dealt with” (*R. v Evans*, 1996, para. 3). To prevent police “fishing expeditions” and protect Canadians from unjustified searches that could expose them to criminal charges without a criminal investigation to properly support those charges, the courts must determine “whether in a particular

situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement" (*Hunter et al. v. Southam Inc.*, 1984, pp. 159-160). With the advent of the Charter, the Supreme Court of Canada extended these protections against territorial trespass, more generally and s.8 of the *Charter* was held to "guarante[e] a broad and general right to be secure from unreasonable search and seizure" (*Hunter et al. v. Southam Inc.*, 1984, p. 167) so that all aspects of private life should be protected from government interference whenever the individual has a reasonable expectation of privacy.

In *R. v. Thompson* (1990), the Court first applied this standard to technologically mediated searches. In the majority judgment, La Forest asserts that "[s]urreptitious electronic interception of private communications constitutes a 'search or seizure' within the meaning of s. 8 of the Charter" (p. 1117) and should therefore be protected as private. However, the nature of electronic information and communications raises new questions about how government regulations should be implemented. La Forest's comments on this are worth quoting in full:

In a modern industrial society, it is generally accepted that many activities in which individuals can engage must nevertheless to a greater or lesser extent be regulated by the state to ensure that the individual's pursuit of his or her self-interest is compatible with the community's interest in the realization of collective goals and aspirations. In many cases, this regulation must necessarily involve the inspection of private premises or documents by agents of the state [...]

The situation is, of course, quite different when the state seeks information, not in the course of regulating a lawful social or business activity, but in the course of investigating a criminal offence. For reasons that go to the very core of our legal tradition, it is generally

accepted that the citizen has a very high expectation of privacy in respect of such investigations. The suspicion cast on persons who are made the subject of a criminal investigation can seriously, and perhaps permanently, lower their standing in the community. This alone would entitle the citizen to expect that his or her privacy would be invaded only when the state has shown that it has serious grounds to suspect guilt. This expectation is strengthened by virtue of the central position of the presumption of innocence in our criminal law. The stigma inherent in a criminal investigation requires that those who are innocent of wrongdoing be protected against overzealous or reckless use of the powers of search and seizure by those responsible for the enforcement of the criminal law. The requirement of a warrant, based on a showing of reasonable and probable grounds to believe that an offence has been committed and evidence relevant to its investigation will be obtained, is designed to provide this protection.” (*Thomson Newspapers Ltd. v. Canada*, 1990, pp. 507-508)

The constitutional standard, therefore, is important precisely because “if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated” (*R. v. Dyment*, 1988, para. 23). However, as Lessig (1999b) points out, digital infrastructures often supersede regulatory models and open up individuals to more and more surveillance as a matter of course. He explains, “[a] regulating standard restricts behavior within that activity, according to a policy set by the regulators” (p. 759) but with digital communication “the architecture of cyberspace is, in effect, a regulator” (p. 762) because it dissolves the lines between public and private. The result is that more and more personal and non-personal data is captured by corporations which can make it available to the state. These indistinct boundaries between

public and private spaces and the vast amount of corporately-held data threaten to shift the balance that we previously relied upon, with significant consequences for police powers.

Three landmark cases explain the courts' interpretation of privacy within the context of modern technologies: *R. v. Plant* (1993), *R. v. Tessling* (2004), and *R. v. Spencer* (2014).

In *R. v. Plant* (1993), the Supreme Court of Canada was asked to decide whether or not police performed an illegal search when they obtained information about a house's electrical consumption in order to infer the presence of a marijuana growing operation within its premises. This case raised questions about the boundaries between territorial and informational privacy. At the time, informational privacy had traditionally been considered less important than territorial privacy, and was therefore held to a lower privacy standard under the legal protection from search and seizure (Bailey, 2008). These standards became more complex as new technologies were developed and "create[d] novel privacy concerns by making knowable and meaningful information and data that previously existed but weren't susceptible to being captured or conclusively comprehended through ordinary human senses" (Bailey, 2008, p. 283). Although *R. v. Plant* (1993) did not pertain to new technologies specifically – the information sought by police was routinely collected as part of the electrical service – it did invoke the vaguely-defined boundary between the physical content of the household and information that could represent the content of the household. In this case, it was clear that the police wanted to find evidence of a marijuana operation, and the electrical records provided the same confirmation they would have obtained by physically entering the house and observing it themselves. The Court found that the search was constitutional and that the appellant had no privacy expectations because the service provider, the Calgary Commission, clearly stated in its policies that it would share information with the police, but the reasons raised several concerns about informational privacy. Justice

McLachlin's dissenting judgment in particular highlighted that the information sought was not widely accessible or publicized, and that it revealed things that were happening inside the house, which potentially implicated territorial privacy:

I conclude that the information was not public, since there is no evidence suggesting that this information was available to the public and the police obtained access only by reason of a special arrangement. The records are capable of telling much about one's personal lifestyle, such as how many people lived in the house and what sort of activities were probably taking place there. The records tell a story about what is happening inside a private dwelling, the most private of places. I think that a reasonable person looking at these facts would conclude that the records should be used only for the purpose for which they were made -- the delivery and billing of electricity -- and not divulged to strangers without proper legal authorization. (*R. v. Plant*, 1993, p. 302)

Additionally, McLachlin argued that “[c]omputers may and should be private places, where the information they contain is subject to the legal protection arising from a reasonable expectation of privacy” (*R. v. Plant*, 1993, p. 303). These comments acknowledged that modern technologies were blurring the distinction between informational and territorial privacy, but the concerns raised were not sufficient to persuade the majority of the Court to seriously interrogate and reevaluate legacy privacy standards that had been established by s.8 of the Charter and previous court cases.

In a similar case, *R. v. Tessling* (2004), the Court concluded that information about a house's internal heat signature that had been obtained by the RCMP using a Forward Looking Infra-Red camera did not constitute an unconstitutional search. In Justice Binnie's view, the images were “more accurately characterized as an external search for information *about* the

home which may or may not be capable of giving rise to an inference about what was actually going on inside, depending on what other information is available” (*R. v. Tessling*, 2004, para 27, emphasis in original) and should therefore not be held to the higher standard of territorial privacy. Binnie acknowledged that if the technology improved and the images grew in quality and accuracy, “courts will have to deal with its privacy implications at that time in light of the facts as they then exist” (*R. v. Tessling*, 2004, para. 29). This assumes that the courts will have an opportunity to revise privacy standards as technology advances, and that they will be able and willing to adjust privacy standards according to the new circumstances. This creates an unclear precedent. Although Binnie also opined that privacy is a normative concept, his judgment continues the slide from (strong) territorial protections to (weak) informational protections.

However, in the context of acknowledging the importance of privacy expectations, Binnie does note that “[t]he *subjective* expectation of privacy is important but its absence should not be used too quickly to undermine the protection afforded by s. 8 to the values of a free and democratic society” (*R. v. Tessling*, 2004, para. 42, emphasis in original) and that “[s]uggestions that a diminished *subjective* expectation of privacy should automatically result in a lowering of constitutional protection should therefore be opposed” (*R. v. Tessling*, 2004, para. 42, emphasis in original). These comments echo Lessig’s (1999a) warning that privacy will become legally depreciated as information becomes increasingly public, yet the *Tessling* decision does not take a strong future-facing stance towards privacy rights and seems to postpone the issue instead.

It is in *R. v. Spencer* (2014) that the Supreme Court begins to confront the substantive changes brought about by new forms of searching and, in doing so, points to the need to carefully examine all legislative changes to existing search and seizure standards. The Court was asked to evaluate the constitutionality of a search that occurred after police obtained client

information from an internet service provider (ISP) in order to identify and find a suspect. The Crown suggested that “permissive” privacy legislation in PIPEDA legitimized the collection of the relevant data. Although the Court agreed that the search was constitutional, it did acknowledge that where privacy rights are concerned, “[t]he analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought” (*R. v. Spencer*, 2014, para 36). By recognizing that “the impact of the search on its target” is an element of privacy, albeit a subjective one, the court acknowledged that the intimacy of information, regardless of the legality of a search, should be taken into consideration when evaluating privacy thresholds. The Court also extended privacy concerns to include anonymity, underscoring the importance of privacy rights to democratic freedoms; the ability to participate in political activity anonymously is important (Mladenov and Galetin, 2025; Pandey, Gupta, and Chattopadhyay, 2020), and so anonymity allows Canadians to protect themselves from illicit state attention by allowing them to express themselves without having to worry about who may be monitoring their speech, as it is not associated with their identity. This establishes a much more flexible and practical privacy standard than the one in *Tessling*, which attempted to set an objective standard based on the quality of technology at a specific point in time.

These three cases implicate the privacy concerns La Forest raises – that seemingly innocuous information obtained without a warrant could expose Canadians to criminal charges that would significantly affect their reputations and lives. Subscriber information held by ISPs is especially concerning because the technological infrastructure required to obtain and provide it to state actors arguably requires the ability to monitor and search all subscribers’ activities,

placing all clients under constant surveillance in case that surveillance is one day required and deemed legally reasonable.

Moreover, the transparency created by surveillance creates an asymmetrical relationship between the state and its citizens. Personal information is exposed to corporate monitoring and searching, but the Edward Snowden leaks revealed that the United States maintained an extensive secret surveillance program in collaboration with private companies (Finley and Esposito, 2014; Kelly, 2022). The secrecy involved made it impossible for citizens to fully understand the government's policies and hold the state fully accountable, which is an important component of the democratic relationship between the state and its citizens (Nyst, 2018). While the State grants itself the authority to place its citizens under surveillance – and suspicion – it does not allow its citizens to know the full extent of the surveillance systems that observe and permeate their lives. Therefore, citizens lack the information necessary to evaluate the surveillance policies that can affect their lives and are partially robbed of their political agency, as their ability to hold the State accountable for the abuses caused by these unknown surveillance measures is limited. This asymmetry in transparency and opacity is the heart of the problem posed by the expansion of modern surveillance.

Canadian Lawful Access Legislation

My project examines these surveillance and privacy issues through the lens of Canadian lawful access legislation. Since the beginning of the 21st century, multiple attempts were made to modernize lawful access legislation in response to the trends discussed above. In this part of the introduction, I provide a brief synopsis of this legislative activity in order to provide context for my research question.

The most important bills started with the *Modernization of Investigative Techniques Act* (Bill C-74, 2005), which was proposed by a Liberal government. It was followed by the *Investigative Powers for the 21st Century Act* (Bill C-46, 2009) and the *Technical Assistance for Law Enforcement in the 21st Century Act* (Bill C-47, 2009), the *Improving Access to Investigative Tools for Serious Crimes Act* (Bill C-50, 2010), the *Investigative Powers for the 21st Century Act* (Bill C-51, 2010), and the *Investigating and Preventing Criminal Electronic Communications Act* (Bill C-52, 2010), the *Protecting Children from Internet Predators Act* (Bill C-30, 2012), and the *Protecting Canadians from Online Crime Act* (Bill C-13, 2013). The details of the legislation changed over the years, especially when certain bills were combined or divided, but their shared purpose was to modify the *Criminal Code* (1985) and other related laws to “modernize” the law and adapt it to new technologies.

According to the text of the legislation, the objective of Bill C-74 was to ensure that telecommunications would have the technical infrastructure required to collect subscriber information and make it available to law enforcement agencies:

The purpose of this Act is to ensure that telecommunications service providers have the capability to enable national security and law enforcement agencies to exercise their authority to intercept communications, and to require service providers to provide subscriber and other information, without unreasonably impairing the privacy of individuals, the provision of telecommunications services to Canadians or the competitiveness of the Canadian telecommunications industry. (Bill C-74, 2005, p.3)

Although there were clauses and exemptions to accommodate smaller service providers who could not develop the required infrastructure and to account for other possible technical difficulties, Bill C-74 made it obvious that the state wanted to take advantage of the monitoring

and searching infrastructure that could be built into telecommunications technologies, echoing the police interest in electricity use seen in *R. v. Plant* (1993). The state believed that subscriber information could be useful to its policing, and it wanted to guarantee that service providers would be able to monitor and record the information for future reference. Corporate surveillance of users was considered an important step towards the modernization of state surveillance.

Bill C-46 (2009) and Bill C-47 (2009) were proposed in 2009 by a Conservative government. Bill C-47 was functionally identical to Bill C-74, while Bill C-46 focused on the lawful access framework that would allow the state to legally obtain information from telecommunication companies. These measures included preservation demands that would allow peace or public officers to ask a person to “to preserve computer data that is in their possession or control when the demand is made” (Bill C-46, 2009, p. 10) for up to 21 days, preservation orders approved by a justice or judge that would extend the time period to 90 days, as well as separate production orders that would allow a peace or public officer to, with the approval of a judge or justice, to demand that a person provide documents containing general data, communication data, transmission data, tracking data, financial data. Furthermore, the bill included checks and balances that clearly limited and defined the circumstances in which documents could be requested and ordered the destruction of irrelevant or unused data.

These unsuccessful bills were followed by Bill C-50 (2010), Bill C-51 (2010), and Bill C-52 (2010), which, collectively, were quite similar to the previous legislation. Bill C-30 (2012) consolidated all the proposed measures, many of which returned in Bill C-13 (2013), which received Royal Assent in 2014 (Bill C-13, 2014).

However, there was one notable exclusion from Bill C-13. Bill C-46, Bill C-50, and Bill C-30 contained the following clause:

487.11 Either a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament may, in the course of their duties, exercise any of the powers described in section 487, 492.1 or 492.2 without a warrant if the conditions for obtaining a warrant exist but it would not be feasible to obtain a warrant because of exigent circumstances. (Bill C-46, 2009, p. 21; Bill C-50, 2010, p. 7; Bill C-30, 2012, p. 58; underline in original to represent changes to the *Criminal Code*.)

In all attempts to modify lawful access legislation, including Bill C-13, section 492.2 pertained to the “[w]arrant for transmission data recorder” (Bill C-46, 2009, p. 24; Bill C-51, 2010, p. 23; Bill C-30, 2012, p. 61; Bill C-13, 2013, p. 28). The legislation further defines a transmission data recorder as “a device, including a computer program within the meaning of subsection 342.1(2), that may be used to obtain or record transmission data or to transmit it by a means of telecommunication” (Bill C-46, 2009, p. 25; Bill C-51, 2010, p. 24; Bill C-30, 2012, p. 62; Bill C-13, 2013, p. 29). That section could have allowed the Canadian government to obtain or record transmission data without a warrant in exigent circumstances, but none of the bills that included it received royal assent.

Instead of section 487.11 cited above, Bill C-13 included the following:

487.0195 (1) For greater certainty, no preservation demand, preservation order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing.

(2) A person who preserves data or provides a document in those circumstances does not incur any criminal or civil liability for doing so. (Bill C-13, 2013, p. 24)

This clause was particularly controversial,² as it raised questions about the role of judicial warrants and whether Bill C-13 allowed for *de facto* warrantless by enabling and perhaps even encouraging voluntary compliance with production orders.

The content of these proposed laws illustrates many of the key issues discussed in this chapter. The legislative focus on the preservation and production of data once again emphasizes the importance of monitoring and searching to surveillance. Preservation demands and orders were meant to guarantee that documents would be available if they were considered necessary to an investigation. Production orders were meant to ensure that data would be made available upon request. There was also a clear, longstanding interest in allowing warrantless access to transmission data in ostensible emergencies. The emphasis on technological infrastructure represents regulatory standards. Moreover, the comingling of corporate infrastructure and state surveillance interests raises doubts about laws such as the *Privacy Act* and *PIPEDA*, which are meant to regulate how personal information is used and shared. Because of all this, lawful access legislation can serve as a point of focus for Lessig's (1999a; 1999b) warnings and for the concerns about the technological erosion of privacy boundaries that were raised in *Plant* (1993), *Tessling* (2004), and *Spencer* (2014).

While courts have struggled to apply existing jurisprudence to new technologies and attempted to set appropriate boundaries to protect Canadians from unlawful searches and seizures, privacy experts argue that legislation attempting to adapt to new technologies by

² The different interpretations of section 487.0195 and its implications are discussed in Chapter 4 and Chapter 5.

“modernizing” lawful access has instead sought to expand access to personal information, thereby maintaining or even exacerbating the unequal relationship between the state and its citizens. Since exposure to government surveillance can, according to the courts, expose Canadians to further police investigation and more intensive state control, this is a subject of great criminological importance.

This thesis will examine these issues by using social problem theory (Kitsuse and Spector, 1973; Kitsuse and Spector, 1975; Spector and Kitsuse, 1973; Spector and Kitsuse, 2017) to analyse the parliamentary debates on lawful access legislation from 2009 to 2013.³ Social problem theory is a theoretical framework that examines how claims-makers rhetorically construct social problems – and their solutions – based on putative social conditions. By using this approach, this thesis will critically analyze how different claims-makers such as politicians, privacy advocates, legal experts, law enforcement officers, and government workers socially constructed lawful access, surveillance, and privacy rights.

Thesis Outline

Chapter 1 provides an overview of the literature on surveillance and privacy, touching upon the historical use of surveillance in Canada, the implications of surveillance and privacy for basic democratic rights, and the risks of cybercrime. It explains the importance of privacy as a democratic right and demonstrates how it has often been subverted because of perceived security risks, providing important context for the analysis of my data.

³ Bill C-74 (2005) is discussed in this chapter and in Chapter 4 due to its historical relevance; later legislation was based on Bill C-74 and that particular bill represents the Liberal Party’s support for lawful access at a certain point in time. During the early stages of analysis, the project began to focus on the legislation discussed from 2009 to 2014 because represented the Conservative government’s ongoing attempts to implement new lawful access legislation.

Chapter 2 explains this study's theoretical framework and research methods. It focuses on the importance of rhetorical constructs as data, defines the key rhetorical elements that served as the foundation of the analysis, and explains how the data was organized, coded, and analyzed.

Chapter 3 discusses how claims-makers constructed modern technologies as a criminal danger to Canadian society. Proponents of lawful access legislation claimed that new technologies facilitated crimes or created new crimes that necessitated new investigative powers – powers that would be made available through lawful access legislation. In addition, privacy advocates also largely agreed with these claims, which created a complex rhetorical relationship of combined support and opposition.

Chapter 4 examines how privacy advocates socially constructed lawful access legislation as a loss of privacy. Claims-makers highlighted the importance of privacy as a democratic right, arguing that lawful access legislation would infringe upon Canadians' privacy and cause significant harm. In spite of this, privacy advocates adopted key elements of the security rhetoric, which made it difficult for them to convincingly express their points.

Chapter 5 studies how proponents of lawful access legislation presented the legislation as a form of privacy protection. They claimed that the legislation contained sufficient oversight to protect Canadians' privacy rights and that the information available through lawful access was not personally significant and would not infringe upon privacy rights.

The conclusion integrates the rhetorical analyses in order to show how Canadian lawful access legislation can provide greater insight into the broader context of surveillance's development. Though the legislation itself exists within the specific legal and political context of Canada, the rhetorics used to construct, defend, and oppose it are similar to the global

discussions about surveillance and privacy that have been ongoing for several years; lawful access legislation can thus be used to better understand how these discussions play out over time.

Chapter 1: Risk and the Expansion of Canadian Surveillance

In this chapter, I examine the state's longstanding interest in accessing private communications. To do this, I adopt David Lyon's (2003) definition of surveillance as "routine ways in which focused attention is paid to personal details by organizations that want to influence, manage, or control certain persons or population groups" (p. 5), which supports inquiry into the many ways that the state has used surveillance as an instrument of everyday social control. Moreover, the definition sits at the base of much of surveillance studies scholarship that has explored how the state's exponentially growing ability to observe, document, measure, and categorize citizens enables new forms of intrusion and control (see Axelrod, 1995; Brown and Brown, 1978; Deleuze, 1995; Finn, 2005; Foucault, 1995; Haggerty and Ericson, 2000; Kealey, 1992; LeRat and Ungar, 2005; Lonardo, 1995; Parnaby and Kealy, 1997; Proulx, 2014; Scott, Tehranian, and Mathias, 2004; Smith, 2010; Thomas, 1994). In particular, Lyon's (2003) emphasis on "routine ways" of surveillance shows how pervasive methods such as wiretapping, i.e. "intercepting a communication while the communication is taking place" (Desai, 2007, p. 556), can be integrated into daily life and allow the state to penetrate private spaces.

In fact, the state's interest in private communications is well-documented. Though there were other factors involved, Desai (2007) links the establishment of the American postal system to the way the 18th century British government used its postal service as an intelligence agency to intercept private correspondence, which made it difficult, if not impossible, for members of the

American revolutionary movement to communicate with residents of other colonies. When the telegraph became widespread, both sides of the American Civil War intercepted enemy telegraph communications to obtain military intelligence (Hochman, 2022), and during the mid-19th century, European governments “took control of telecommunications as a matter of national security and joined together via multilateral treaty to establish transcontinental interconnection” (Hills, 2006, p. 197), and Article 19 of the Convention Télégraphique Internationale de Paris (1865) stipulated that the countries could stop private telegram transmissions that were deemed a threat to their national security.

These practices grew as telegraphy was overtaken by telephony. Molinaro (2017) discovered that, in 1951, Canada secretly established the PICNIC program, a large-scale wiretapping project. In addition to authorizing surveillance, PICNIC included stipulations that “[a]ny law, criminal or otherwise, could be violated if it was done to carry out wiretapping” (Molinaro, 2017, p. 466), allowing government agencies – and the communication companies that would necessarily cooperate with them to implement the wiretapping – to act outside the bounds of the law without repercussion.

Today, communication and technology companies routinely collaborate with American intelligence agencies to intercept communications (Finley and Esposito, 2014). However, as communication technologies have globalized and become more accessible to the general public, governments have enjoyed easy access to a growing number of private messages. As Lyon (2003) and Mathiesen (2013) note, the surging fear of terrorism after 9/11 accelerated the expansion of state surveillance of electronic communications, but the practices themselves were well established before then. Accordingly, lawful access legislation is contextualized within this broader historical trend. While this research project focuses on the surveillance of modern

technologies, it is clear that the state logic that legitimizes – or demands – the surveillance of private communications has persisted for well over one hundred years. The modern state, which Nasu (2015) describes as the “national security state” (p. 366), merely intensifies and expands upon what was already there.

Much of surveillance studies scholarship has linked this trend to issues such as cybercrime (see Akdeniz, 2002; Etter, 2001; Pallaras, 2011) and terrorism (see Lyon, 2003; Mathiesen, 2013), which have become the “national security concerns” that justified the state’s desire to intercept letters, telegrams, and phone calls in the past. Because of this, the debates surrounding surveillance and privacy have focused on the need for “balance” between security and civil rights (see Baker, 2003; Bannister, 2005; Neocleous, 2007). Legal privacy rights are weighted against national security risks and, when the state deems it appropriate, they are curtailed accordingly.

The prioritization of security over rights has become increasingly problematic because of the way modern telecommunication technologies combine instant communications and permanent records that can easily be searched, something which past technologies could not achieve. Lessig’s (1999a) analysis of surveillance argues that it is now easier to monitor personal activities and communications and to search the records that have been produced by monitoring, as seen in the clauses of lawful access legislation that compel telecommunication service providers to build infrastructure that would allow them to preserve communications and customer information so that it would remain available to police. Surveillance of the post requires physical access to a letter and is only possible if there is a way to identify suspicious letters. Telegraph surveillance requires physical access to the telegram or a wiretap. Phone surveillance requires real-time monitoring. Once the window is closed – the letter or telegram

has been delivered, the phone call is over – surveillance becomes impossible. Modern technologies avert this:

The architecture of cyberspace can be such that collecting data is the default. The world there can be made such that in the ordinary case, information is collected ceaselessly-invisibly, behind the scenes, efficiently, with no burden on the user. The information is collected; it is more easily searched; and the legal protections against its search – protections grounded in the burden that a search would create – disappear (Lessig, 1999a, p. 62).

Modern technologies combine communication and surveillance, making the two nearly indistinguishable. The window of opportunity for surveillance is not an obstacle to practical surveillance and information is retained so that it can be referenced in the future if needed.

The continuous, routinized nature of surveillance in modern society raises concerns about how the collected information could be used, especially by the state. In *Thomson Newspapers Ltd. v. Canada* (1990), La Forest emphasizes that privacy rights are necessary because unwarranted state intrusion can expose Canadians to criminal investigations and the associated stigma. Furthermore, Smith (2009) argues that “[w]hile intelligence-gathering modes may appear neutral, their effects caused and justified a range of discriminatory treatment” (p. 16), so there is a very real possibility that the surveillance used to “impartially” search through communications could perpetuate biases, inequality, and discrimination against people who have committed no crimes and pose no threat to public safety.

The potential abuses of surveillance are furthered magnified by the state’s interest in managing risk, the factor that underlies cybercrime, terrorism, national security, and the balance

between security and privacy and civil rights. Risk-focused governments “produc[e] the crucial categories of suspicion within which individuals may be located but where their voice is muted” (Lyon, 2003, p. 45) and establish “norms that emphasize a future-orientation involving control patterns over whole categories of people and which develop risk profiles for entire groups” (Mathiesen, 2013, p. 99) in order to identify potential threats to society and protect national security. Combined with the ubiquitous and unobtrusive surveillance mechanisms that are included in modern telecommunication technologies, this places citizens in a state of constant suspicion, and civil privacy rights that would prevent the state from accessing private information or communications become a risk themselves.

Several examples of how the Canadian state used surveillance in the past lends credibility to these fears. Canadian colonialism made extensive use of surveillance to police First Nations and Indigenous peoples (Proulx, 2014; Crosby and Monaghan, 2016; Howe and Monaghan, 2016), police spied on “Communist” labour organizations that were active during the first half of the 20th century (Axelrod, 1995; Kealey, 1992; Lonardo, 1995; Parnaby and Kealy, 1997), the federal government of the 1950s and 1960s used surveillance to identify gay and lesbian employees of the civil service so they could be removed (Kinsman, 1995). More recently, this same trend was active after the 9/11 terrorist attacks; national security surveillance quickly expanded beyond terrorist threats to encompass whole communities, perpetuating and amplifying islamophobia and anti-Muslim discrimination (Jamil, 2017; Nagra and Maurutto, 2016). The groups were targeted by these surveillance measures because they were considered threats to national security – or rather, “national security” was defined in a way that interpreted these groups and individuals as a threat to the nation on the basis of their cultural identity, political

beliefs, sexual orientation, or religion, not because they posed a threat to life or public safety. Again, La Forest's concerns about privacy and state intrusion are validated.

Furthermore, modern technologies have significantly altered the way the government approaches putative risks to national security. As societies have shifted from what Foucault (1995) calls disciplinary power – the ability to exert power through highly-visible surveillance mechanisms and closed institutions that can easily regulate the time and space within their walls – to what Deleuze (1995) describes as a control society – a far less obvious and obtrusive system of surveillance that relies on rapid communication to track the movement of individuals through different social institutions and constantly confirm their identities and their level of access to institutional services – individuals' private communications and information have become increasingly exposed. The historical surveillance methods Foucault examined, such as Bentham's panopticon (Bentham and Božovič, 1995), were based on closed institutions that were relatively easy to observe and control. In these institutions, individuals who were considered a risk to society could be supervised and eventually released when they were deemed safe. Conversely, the control society functions because institutions are *open* to constant movement and access, and "risky" individuals are considered so because they are participating in the routine activities of society. Framed in the context of Lessig's (1999a, 1999b) arguments about the way modern technologies facilitate monitoring and searching, devalue privacy as a legal concept because of the way it is interpreted by the courts, and allow the government to regulate means of communication, the institutions of the control society – such as telecommunication service providers – operate on the basis of constant surveillance and become part of the state's surveillance regime themselves. Though lawful access legislation regulates government access to communications through restrictions, warrants, and legal orders and demands, the fundamental

surveillance system is universal and indiscriminate by necessity. Otherwise, there would be no information to target with preservation orders or demands in the first place. Lawful access therefore becomes an important moment to scrutinize because it seeks to impose a socio-technical frame around the state's ability to place its citizens under surveillance that is naturalized as it recedes into the technical infrastructure.

The way modern technologies routinely intercept communications and gather information raises concerns about the risk-focused state's approach to policing, national security, and privacy rights. To place my analysis of lawful access in this context, I now provide a more detailed analysis of how the Canadian state's pursuit of national security has led to discriminatory policies in the past. Following this, I explore how surveillance regimes have expanded in space and time through international agreements and preventative intervention. Finally, I discuss privacy issues to highlight the growing democratic gap between the state's surveillance regime and control over information and policy, on the one hand, and individuals' privacy interests and desire to control their personal information and communications on the other.

Surveillance and the Canadian Identity

On several occasions in Canadian history, the state has implemented surveillance measures and discriminatory policies in the name of national security. To start, surveillance was an integral part of the Canadian state's colonial project during the 19th and early 20th century (Monaghan, 2013; Smith, 2009). According to Smith (2009), this surveillance was primarily overseen by the Department of Indian Affairs and police agencies, with the support of religious missionaries from various denominations, government officials from other departments, politicians, Canadian settlers, other private individuals, and even Indigenous people who had been recruited for this purpose. The purpose of this surveillance was to "provide a portrait of the

progress of colonial rule” (Smith, 2009, p. 17) and establish a colonial system in which “[t]he perceived attributes of Whiteness, Protestantism, and British heritage were the reference points for normality against which all was judged” (Smith, 2009, p. 18). In this context, “the anxieties of white administrators and settlers were amplified based on racialized stereotypes and fears of nomadic, illiberal, and vengeful outsiders hedged against European civilization” (Monaghan, 2013, p. 495). At the time, the state believed that “colonial surveillance practices necessitated a vigilant gaze towards traces of indigeneity that marked deviant behaviour from, or dangerous threats towards, the expansion of settler governance” (Monaghan, 2013, p. 488). Colonialism was the national security policy of the time, and Indigenous people were the national security risk that had to be observed and policed. This risk was not to life, but to the continued expansion of the colonial settler state based on European culture and norms.

This colonial surveillance has persisted across time. Modern policing and surveillance programs have at times reinterpreted Indigenous activism as a criminal or terrorist threat (Crosby and Monaghan, 2016; Proulx, 2014) that needs to be controlled. According to Monaghan and Walby (2012), “intelligence agencies have blurred the categories of terrorism, extremism and activism into an aggregate threat matrix” (p. 134), which effectively expands the definition of national security risks to include legitimate forms of political activity and, when applied to the context of Indigenous activism, replicated the same surveillance logic that was used during Canada’s colonial expansion. Similarly, Lyon (2003) argues that laws meant to protect people from terrorism have been used to monitor and arrest activists, and Mathiesen (2013) shows that European counterterrorism laws are vague enough to bring a wide number of activities which are not harmful to public safety into the surveillance net. Though protest and political activism are

necessary political freedoms in a democratic state, they are often confounded with national security risks in troubling ways.

Overbroad definitions of “national security” have also discriminated against Canadians on the basis of their personal political beliefs or their sexual orientation. During the early decades of the 20th century, the Canadian government spied on “Communist” organizations often associated with the labour movement (Axelrod, 1995; Kealey, 1992; Lonardo, 1995; Parnaby and Kealy, 1997). From this perspective, labour movements, which were expected to support capitalism, were reconstituted as a risk to (capitalist) national security. Later, during the 1950s and 1960s, the government identified and terminated the employment of gay and lesbian employees of the civil service on the basis that their sexual orientation made them vulnerable to blackmail (Kinsman, 1995). Although these employees were not directly discriminated against due to their sexual orientation, they were considered a threat to national security because their sexual orientation was considered a form of deviance from heteronormativity that could be leveraged as a means of blackmail; placing them under surveillance and terminating their employment made the state an enforcer of heteronormativity, in spite of the fact that the people targeted had committed no crime and did not pose a threat to life or public safety. They were, at most, a *potential* intelligence vulnerability, yet the state’s risk management strategy required that this potential vulnerability be pre-emptively eliminated.

More recently, following the 9/11 terrorist attacks, Muslim Canadians were subjected to a similar treatment when “long-time, peace-loving, contributing citizens and residents were being viewed as potential enemies and terrorists by virtue of their race, ethnicity, and religion” (Hanniman, 2008, p. 273). It has also been found that the surveillance of air travel “contributes to Islamophobia through disproportionately profiling racialized Muslim and Muslim-looking

passengers as members of a suspect community” (Jamil, 2017, p. 74) and young Canadian Muslims also faced more discrimination at the borders (Nagra and Maurutto, 2016). Although this did not occur in the context of colonialism, the parallels between the surveillance of Indigenous people who were considered a threat to the colonial state’s expansion and the Muslims who were considered a threat to the globalized Canadian state now are there; the persistent racialized aspects of this become more explicit in light of “secular” political movements that indirectly and directly position themselves against Islam and Muslim Canadians while endorsing white, Christian, European social norms (see Stonebanks, 2019). Though terrorism was the primary national security threat targeted by these measures, the measures certainly had unintended consequences for innocent Canadian citizens who were stigmatized as potential criminals, much like La Forest warned, due solely to their religious beliefs.

These discriminatory practices are being embedded into emerging artificial intelligence (AI) surveillance systems, where, according to McQuillan (2022), false positives and false negatives have serious “unintended” consequences for the individuals wrongfully labelled as a risk due to AI’s discriminatory biases and inability to understand causality beyond a superficial sense. In fact, it seems that surveillance for surveillance’s sake is one of the priorities of counterterrorism laws; for example, the National Security Entry-Exit Registration System established by the United States in the aftermath of the 9/11 terrorist attacks “functioned less to enhance border security, than to code, categorize and display certain bodies as potentially threatening and as warranting continued surveillance” (Finn, 2005, p. 140). Similarly, the benefits of Europe’s Schengen Agreement, such as freedom of movement within Europe’s borders, are primarily enjoyed by people with *European* citizenship (Maas, 2005), not to provide fair and equal rights for all. Likewise, the increasing use of AI tools in criminal investigation (see

Faqir, 2023) and intelligence gathering (see Vogel, Reid, Kampe, and Jones, 2021) raises doubts about the fairness of surveillance systems, especially in light of some of the biases that are often perpetuated by surveillance or the national security state (see Crosby and Monaghan, 2016; Finn, 2005; Hanniman, 2008; Jamil, 2017; Lyon, 2003; Maas, 2005; Mathiesen, 2013; Monaghan and Walby, 2012; Nagra and Maurutto, 2016; Proulx, 2014;). The integration of AI in preventative intervention in crime and national security therefore poses a threat to the fundamental principles of investigative standards, thresholds of suspicion, and due process – especially if AI is ever added to the surveillance infrastructure required by lawful access and becomes responsible for intercepting and identifying “risky” communications.

These cases clearly show the importance of La Forest’s warning that citizens should be protected from unjustified state intrusion (*Thomson Newspapers Ltd. v. Canada*, 1990). When the Canadian state injects itself into the lives of Indigenous people or Muslim Canadians or workers whose political beliefs diverge from mainstream economic policies, it is to portray them as a security risk. In particular, the discrimination against LGBTQ+ members of the public service because they could be vulnerable to blackmail illustrates how the prioritization of national security over civil rights can implicate individuals who have broken no laws and pose no credible threat to general public safety. The costs of national security have historically been paid by the individuals who were stigmatized by state surveillance.

Because of this, lawful access legislation should be approached with caution. Though it purports to update Canadian law and investigative procedures to adapt them to new technologies, Canada’s history with surveillance reveals that the definitions of “national security” and “risk” have often been broadened beyond physical threats to public safety. The possibility that lawful

access could introduce these biases into Canada's telecommunication infrastructure should be evaluated.

The Extension of Surveillance in Space and Time

In this section, I examine the relationship between risk and the extension of surveillance in space and time. It is well established that states have responded to the risk of terrorism by expanding their surveillance and security measures (Baker, 2003; Nasu, 2015; O'Brien, 2009; Yoo, 2014). The 9/11 terrorist attacks in particular were used justify the expansion and acceleration of pre-existing surveillance trends (Lyon, 2003; Mathiesen, 2013), highlighting the ongoing debates between national security and civil rights (Baker, 2003) that have often prioritized security (Lyon, 2003; Mathiesen, 2013). However, these policies also challenge the notion of space and time as they relate to the state's authority and jurisdiction. In the words of Baker (2003), states' battle against terrorism "is bound neither by time, geography, nor specific adversaries" (p. 548). This has implications for lawful access because, by implementing surveillance infrastructure in law, it makes certain private spaces and communications accessible to the state and defines when and for how long they can be observed or recorded; per Lessig (1999a), modern technologies preserve transient moments in potentially permanent records, so it can no longer be assumed that private activities or communications will be kept within a private physical space or fade over time. In the modern surveillance infrastructure, space and time are no longer obstacles to observation.

Firstly, states have used the risk of terrorism to conjoin domestic and foreign policy in matters of national security, which has significantly increased the geographic reach of state power. In the United States, the risk of terrorism allowed the White House to centralize power due to the presidential office's greater control over international relations and military

interventions (Baker, 2002; Baker 2003). More overtly, the “War on Terror” was used to justify military intervention in Afghanistan (Sahill, 2019), Iraq (Krebs and Lobasz, 2007), and all over the globe (Ryan, 2011), and to establish carceral institutions in foreign areas such as Guantanamo Bay, Cuba, and Abu Ghraib, Iraq (Adams, Balfour, and Reed, 2006). The American government accordingly extended its reach across borders and acted on a global scale, all in the name of securing its national security against terrorism. Its national security policy is therefore no longer restricted to domestic spaces.

Secondly, states have used terrorism as an excuse to shift temporally “from *response to prevention*” (O’Brien, 2009, p. 904, emphasis in original). States now argue that the risk that insufficient intelligence would lead to more terrorist strikes (Finley and Esposito, 2014) requires a general response that “involves aiming for earlier thresholds of detection of terrorists or foreign agents in order to conduct surveillance on and generate further intelligence leads” (O’Brien, 2009, p. 904) in order to more effectively identify potential threats before an attack occurs. The urgent desire to identify risks ahead of time is relevant to the expansion of surveillance, as surveillance is required to act preventatively; this shift in time can also be seen in the carceral measures that states have adopted in response to terrorist threats, such as Australia’s preventative detention orders, prohibited contact orders, and control orders (Ananian-Welsh, 2015; Chetty, 2016; Fairall and Lacey, 2007) which can be used to detain individuals without formal charges or restrict their freedoms of association or movement if doing so would – allegedly – prevent a terrorist act in the future. The preventative detention order regime in particular “is a form of executive detention which allows an individual to be held in custody for up to 168 hours without being charged with a crime (or even suspected of committing a crime) where holding the individual would assist the Australian Federal Police (‘AFP’) or the Australian Security

Intelligence Organisation (‘ASIO’) in a terrorist investigation” (Chetty, 2016, p. 88). This essentially allows the Australian state to pre-emptively utilize punitive carceral measures as preventative measures without establishing guilt. In the words of Baudrillard (1994), simulation – in this case, the simulation of risk – has become “the generation by models of a real without origin or reality; a hyperreal” (p. 1) that allows the state to eliminate the distinction between present crime and the possibility of a future risk and provides the justification required to expand the state’s temporal window of intervention.

As for the risks that are often associated with cybercrime, they are based on several different claims about technological problems and limitations that are used to justify the surveillance of online spaces: the anonymity of the internet (Akdeniz, 2002; Armstrong and Forde, 2003; Rohret and Kraft, 2011); the technical complexity of digital evidence (Broadhurst, 2006; Chaikin, 2006); the multijurisdictional nature of electronic criminal activities that seamlessly cross borders (Brenner, 2006; Calderoni, 2010; Clough, 2012; Speer, 2010); and the opaqueness of the Dark Web marketplace (Shillito, 2019). Additionally, there are concerns that telecommunication technologies have made it easier to commit old crimes such as scams (Pallaras, 2011) and created completely new crimes based on disrupting computer services or accessing private data illegally (Etter, 2001), further expanding the putative gap between modern criminal capabilities and laws that were written for a different – and now “outdated” – technological context.

According to the state, each of these risks makes it more difficult to investigate and then prosecute computer-related crimes, either because the technology itself creates obstacles, such as the anonymity of the internet and the opacity of the Dark Web, or because the law has not yet adapted to new global telecommunication technologies that could easily cross jurisdictions. This

relates to the asymmetrical treatment of new technologies within the state's discourse, and the way it justifies state surveillance. As discussed previously, new technologies extend the reach of state surveillance through space and time (see Baker, 2003; Lessig, 1999a). Yet, criminals' ability to commit crimes on a global scale – their ability to act without spatial boundaries – is considered problematic, while the anonymity and opacity offered by the internet are considered problematic. Examining state surveillance through the way new technologies are constructed as risks reveals the state's sense of entitlement to information; aspects of new technologies that obstruct state access are categorized as risks that need to be mitigated. Thus, the framing of new technologies as obstacles to state surveillance creates a counter-trend that is used to justify the expansion of surveillance. Where and when technologies are used to escape the state's reach, they must be brought within the state's reach to reduce risk.

Given this potent mix of terrorism, cybercrime, and online opacity, states argue that national security can no longer be addressed purely domestically; as Nasu (2015) writes, “the transnational nature of terrorist threats, and the resulting need for greater international cooperation in intelligence gathering and sharing, means that the security of one State cannot be separated from the security of others” (p. 373). Certainly, international policy instruments like the Council of Europe's *Convention on Cybercrime* (2001) is seeking to create international standards of surveillance, which “requires participating nations to enact legislation that facilitates investigation and prosecution of crimes committed through the Internet” (Huery and Rosenberg, 2004, p. 597). The *Convention* argues that, by doing this, states can better address crimes related to new technologies (Glennon, 2012; Jurich, 2008; Lentz, 2010; Huey and Rosenberg, 2004;). Ogasawara (2022) argues that a more careful analysis of Canada's surveillance regime indicates that this global trend calling for “serial legislation has been increasingly legalizing previously

illegal mass surveillance activities that target people inside and outside Canada, particularly involving their personal data through digital networks” (Ogasawara, 2022, p.319). The groundwork for this was laid long ago. Although the *Convention* was signed in November 2001, shortly after the 9/11 terrorist attacks, work began in 1997 (Convention on Cybercrime, 2001), which is consistent with my earlier claim that state surveillance was already expanding years before terrorism became such a prominent concern. Once again, Canadian efforts to enact lawful access provisions in keeping with the *Cybercrime Convention* are accordingly ripe for analysis.

In addition to requiring legislative regimes from its signatories, the Convention “places obligations upon [internet service providers] that, in effect, convert service providers into integral cogs in the apparatus of online law enforcement” (Huey and Rosenberg, 2004, p. 597), blurring the line between private services and public law enforcement and granting the state easier access to the private spaces and communications of the internet. The danger posed by the collaboration between the state and service providers became a major issue in 2013, when whistleblower Edward Snowden revealed that the American National Security Agency (NSA) routinely tapped telephone communications, including those of world leaders (Ball, 2013). The leaks revealed the extensive relationship between state actors and private sector companies such as social media sites and technology companies (Fuchs and Trottier, 2017; Kelly, 2022) and showed how widespread states’ ability to intercept communications was (Fuchs and Trottier, 2017). In like vein, Huey and Rosenberg (2004) argue that the *Convention on Cybercrime* is problematic in part because its articles “demand that signatories enact and use legislation that permits public policing agencies to co-opt internet service providers into being willing or unwilling informants against us, in some situations without prior judicial review” (p. 603-04). Similarly, Finley and Esposito (2014) comment that “[t]he fact that the US national security

functions have been delegated increasingly to corporations reflects a wider pattern of privatization and deregulation that has been gaining momentum since the Reagan administration” (p. 187). Furthermore, as the agreements between states and companies “are financially lucrative to the telecommunications companies with whom the state is partnering” (Finley and Esposito, 2014, p. 189), the companies are incentivized to cooperate with the state’s demands for surveillance instead of protecting the privacy of their customers. A close analysis of lawful access laws will accordingly shed light on this broader trend of privatization and deputization of private sector tech companies.

This model of surveillance as a network of public and private affordances is similar to what Haggerty and Ericson (2000) describe as the surveillant assemblage:

This assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct ‘data doubles’ which can be scrutinized and targeted for intervention. In the 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 (Haggerty and Ericson, 2000, p. 606).

The assemblage envisioned by the *Convention on Cybercrime* ensures that surveillance technologies are neither discrete nor isolated. They are part of a global system of legislation, networked technologies, and standardized investigate procedures meant to extend surveillance capabilities in space and time, detect and prevent risks, and access private digital spaces and communications.

Lawful access legislation is worth studying precisely because it brings Canada into this international surveillance regime by implementing the articles of *Convention on Cybercrime* in Canadian law. Through the enforced collaboration between the state and service providers, lawful access has the potential to establish a ubiquitous surveillant assemblage capable of routinely intercepting private digital communications for preventative purposes that have become associated with detention without guilt or charges. Additionally, the international nature of the *Convention* makes it possible that the communications of Canadians – or of anyone using Canadian communication infrastructure – will be shared with foreign countries.

Democratic Implications of Opacity and Transparency

Lawful access is also a key area for inquiry because international agreements, preventative measures, and surveillance regimes designed to expose the private lives of citizens are frequently accompanied by state secrecy in a way that unbalances the democratic relationship between citizens and the state. According to the state's logic, its policies must "ensure greater government control of information, fewer procedural protections for people linked to terrorism (as either suspects or material witnesses), and enhanced government surveillance" (Baker, 2003, p. 549) in order to prevent terrorist attacks. Conversely, Steeves (2008) argues that the legal test used to determine privacy "is out of step with what we know about people's online experiences and expectations" (p. 334) in a way that exposes citizens to state surveillance and erodes democratic relations. Evolving technologies and anti-terrorism laws make it difficult to determine how reasonable expectations of privacy should be defined (Shade, 2008), yet lawful access legislation offers an opportunity to study how the balance between security and civil rights is rhetorically negotiated. This is especially important because of the potential conflict between the state's pursuit of surveillance and secrecy and the citizens' privacy interests.

As noted above, the Snowden leaks gave the public a glimpse into how extensive the United States' surveillance regime was (see Ball, 2013; Fuchs and Trottier, 2017; Kelly, 2022). These revelations generated a great deal of controversy worldwide (Finley and Esposito, 2014), and they were not met with universal approval; Sagar (2015), for instance, argues that Snowden's actions were fundamentally undemocratic because they violated security measures which were put in place by a democratically elected government, which raises questions about state secrecy within democratic regimes.

Although the surveillance programs Snowden revealed were implemented by democratically elected governments, this does not necessarily mean that they can be considered democratically legitimate. As Nyst (2018) argues, policies can only truly be democratic when voters are in a position to understand what their government is doing and hold elected officials accountable for their policies. However, Snowden exposed surveillance programs that were not publicly known. It would therefore be impossible for voters to evaluate their legitimacy and pass electoral judgment upon the politicians who developed these policies without a whistleblower. Similarly, Nasu (2015) notes that, while freedom of information laws have increased in recent years, "the enactment of specialized State secrets legislation has regained precedence" (p. 370). The surveillance measures put in place by the national security state allow the government to gather information about citizens, but the actions and communications of the state are not made accessible to the public.

The opacity of the state and the (unwilling) transparency of the citizens create an uneven distribution of power that privileges the state. Nasu (2015) further claims that the "over-classification of government information on ever expanding national security grounds has raised concerns about its impact on freedom of information, and the government's public accountability

more generally” (p. 366). These sentiments are echoed by Tigar (2014), who believes that “fundamental principles about restraints on state power are being and have been undermined” (p. 137) and by Finley and Esposito (2014), who describe national security measures as “illegal actions” (p. 191) justified by public fears. According to Nyst (2018), governments are creating “legal frameworks that embed technical capabilities in layers of secrecy and opacity, rolling back hard-won legal protections and removing surveillance from the jurisdiction of accountability and redress mechanisms” (p. 9). These legal frameworks are compounded by the state’s desire to “restrict the right of the public to have access to certain official information [and] impose obligations upon government officials not to make that information public” (Nasu, 2015, p. 371). This secrecy is a direct threat to civil rights and democracies because it obfuscates government policies and makes it difficult for citizens to hold elected officials accountable for those policies.

In addition to this, the ambiguous language often used in surveillance legislation “undermines the clarity and foreseeability of law that is a necessary component of a human rights-compliant surveillance framework” (Nyst, 20018, p. 19) and further threatens “the right to a fair trial, equality before the law and the right to an effective remedy for human rights violations” (Nyst, 20018, p. 19). Citizens cannot assert or defend their legal rights if they do not clearly understand how these rights are applied – or circumvented. This is especially true because of the way lawful access allows surveillance to operate through commercial relationships that would not normally involve the direct intervention of the state, making the surveillance more opaque and difficult to notice. It seems that, at every step, state surveillance seeks to subvert the democratic relationship between citizens and their government.

In contradiction to the state’s secretive expansion of surveillance, individuals expect their privacy to be respected. For example, even as people publicize more and more information about

themselves on social media sites (Steeves and Piñero, 2008), young people also use the internet to communicate in more private ways that their parents and peers cannot overhear (Livingstone & Bober, 2003; Wing and Steeves, 2005) or take steps to prevent their parents from accessing their social media pages (West, Lewis and Currie, 2009). This clearly shows that privacy on networked platforms can be a complex and highly contextual issue (Glac, Elm, and Martin, 2014; Martin, 2012;). In spite of this, law enforcement agencies have demonstrated a clear interest in gathering personal information posted on social media (Egawhary, 2019; Trottier, 2015), an implicit acknowledgement that these communications contain important information about social media users that law enforcement considers relevant. Therefore, social media communications cannot be dismissed as trivial or unimportant, and their privacy interests should be carefully evaluated.

More broadly, privacy from the state is critical to democracy and civil liberties (Andrejevic, 2007; Mathiesen, 2013; Nyst, 2018). The basic concept of privacy carries with it “connotations of the personal, of secrets, and of intimacy” (West, Lewis and Currie, 2009, p. 616) that transcend mere protection from state surveillance and as Moore (2011) argues, privacy “is necessary for human well-being or flourishing” (p. 142). Such privacy standards should be applied to new technologies, and theoretical models such as Communication Privacy Management Theory (CPM) (Petronio, 2013) offer a framework that can be used to understand modern privacy interests.

Within CPM, communication privacy is based on privacy ownership, privacy control, and privacy turbulence. The sense of privacy ownership “defines the boundaries surrounding the information, marking it private” (Petronio, 2013, p. 9), while privacy control is “the engine that regulates conditions of granting and denying access to private information” (Petronio, 2013, p.

9). Together, privacy ownership and privacy control determine what information is considered private and who is authorized to share that information with others. Privacy turbulence occurs when privacy regulation fails to some degree (Petronio, 2013) and makes information available to people who are not authorized to access it. Through this framing, CPM presents privacy as a matter of agency, and loss of privacy equals the loss of agency. Similarly, Austin (2012) suggests that the law should adapt to new surveillance technologies by developing a richer understanding of the core legal principles used to provide privacy with legal protection in the first place rather than focusing on narrow protections from unlawful search and seizure. Lawful access legislation provides an opportunity to consider these issues, but in a surveillance regime predicated on an international reach, preventative intervention, constant suspicion, and state secrecy, it appears unlikely to do so.

Conclusion

The national security state's focus on risk management through surveillance poses multiple problems for civil rights, especially privacy rights, and for the democratic relationship between the state and its citizens. Historically, "national security" and related issues have been interpreted in a broad manner that legitimized state discrimination based on Indigenous identity (Smith, 2009; Monaghan, 2013; Proulx, 2014; Crosby and Monaghan, 2016; Howe and Monaghan, 2016), political beliefs (Kealey, 1992; Axelrod, 1995; Lonardo, 1995; Parnaby and Kealy, 1997; Lyon, 2003), sexual orientation (Kinsman, 1995), or religion (Nagra and Maurutto, 2016; Jamil, 2017). It is clear that broad definitions of national security can be used to target individuals who do not pose a credible threat to the public and only seek to engage in legitimate activities (Monaghan and Walby, 2012; Mathiesen, 2013), potentially allowing the state to place individuals under police control without a valid reason.

In modern Canada, lawful access is at the heart of this problem. Though states have intercepted communications via the post (Desai, 2007), telegraph (Hills, 2006; Hochman, 2022), or telephone (Molinaro, 2017), modern telecommunication technologies greatly facilitate both observation and recording (Lessig, 1999a) and enable surveillance on a scale that would not be practical with older forms of communication. Lawful access takes advantage of this by demanding that private sectors adopt infrastructure that would allow them to monitor their clients and users, preserve data, and provide records to law enforcement upon request. Such cooperation between the state and the private sector is a common practice (Finley and Esposito, 2014; Fuchs and Trottier, 2017; Kelly, 2022) and exemplifies how surveillance has become diffused and ubiquitous within society. Individuals who utilize modern telecommunication technologies are, as a matter of course, placed under constant surveillance by these services.

This extension of surveillance into private spaces of communication is accompanied by the extension of surveillance across national boundaries and time. While international agreements seek to standardize surveillance and investigative practices (Huey and Rosenberg, 2004; Jurich, 2008; Lentz, 2010; Glennon, 2012), the shift in priorities towards preventative intervention over response after the fact (see O'Brien, 2009) leverages surveillance system to identify potential risks before they can become a present danger to society. Yet, the potential use of AI to interpret increasingly large quantities of surveillance data increases the possibility of system errors or outright discriminatory practices (see Finn, 2005; Maas, 2005; McQuillan, 2022) that may criminalize individuals who do not pose a factual threat to public safety. Though lawful access contains limitations and oversight measures that are supposed to avert such problems, governments are becoming opaquer and more secretive in matters of surveillance and

national security (Nasu, 2015; Nyst, 2018), which makes it difficult, if not impossible, for citizens to know for certain that these laws are being respected and enforced.

The issues that surround the surveillance regime of lawful access are defined by their rhetoric: about risk, about national security, about surveillance, about civil rights, about privacy, and about terrorism. They are discursively constructed by various claims-makers who seek to define the appropriate balance between security and civil rights, the criteria that are used to justify suspicion and surveillance, or appropriate privacy protections. Although a practical analysis of lawful access' implementation and use could study its effects on the population, an analysis of lawful access' surrounding rhetoric can better understand how it was developed and established in the first place.

For this reason, this project focuses on the rhetorical evolution of lawful access legislation until it was ratified and became law. To do this, I examine the claims (see Toulmin, Rieke and Janik, 1984) made about lawful access based on their putative factual grounds, justifying warrants, and conclusions, and frame them in the context of social problem theory (see Best, 1987; Best, 2003a; Best, 2003b; Bogard, 2003; Holstein and Gubrium, 2013; Holstein and Miller, 2013; Spector and Kitsuse, 1973; Spector and Kitsuse, 1987) to examine how lawful access and its adjacent issues – such as security and privacy – were rhetorically constructed and contested by various claim-smakers. This theoretical framework allows me to see how lawful access legislation evolved over the years and how arguments for or against it changed.

Chapter 2: Theoretical Framework and Methodology

This chapter establishes the theoretical framework I used to examine lawful access legislation. As discussed previously, the modern surveillance regime is framed by a rhetorical process where issues such as cybercrime (Akdeniz, 2002; Etter, 2001; Pallaras, 2011), terrorism (Lyon, 2003; Mathiesen, 2013), and the balance between security and civil rights (Baker, 2003) are discussed, mobilized, contested, and negotiated. As surveillance technologies spread internationally (see Huey and Rosenberg, 2004; Nasu, 2015), it is important to understand how states mobilize risk and security threats to legitimize increasingly prevalent surveillance regimes. To understand this problem, I decided to base this research on Kitsuse and Spector (1973)'s theory of social problems, which has a unique theoretical perspective on the way problems are socially constructed by the rhetorical activities of invested parties.

Contemporary social problems theory is based on the theory of social constructionism (Best, 1987; Best, 2003a; Best, 2003b; Bogard, 2003; Holstein and Gubrium, 2013; Holstein and Miller, 2013; Spector and Kitsuse, 1973; Spector and Kitsuse, 2017) and emerged in response to epistemological and ontological debates about the relative merits of examining social problems as an objective or subjective field of inquiry. Early studies of social problems are generally based on the functionalist perspective or on value-conflict theory (Kitsuse and Spector, 1973). From the functionalist perspective, Merton and Nisbet (1971) argue that, in order to study social problems, it is necessary to examine objective social conditions which disrupt society. On the other hand, value-conflict theorists such as Fuller and Myers (1941a, 1941b) argue that, in order to study social problems, it is necessary to examine both objective social conditions *and* the public's subjective experience of these conditions; from this perspective, social conditions are only problematic from a sociological perspective if they are also considered problematic by society.

Kitsuse and Spector (1973) critique both approaches, arguing that the functionalist perspective puts too much emphasis on the researcher's role in defining social problems, while the value-conflict theory's insistence on studying subjective *and* objective factors limits its potential. They argue that researchers should define social problems according to “subjective elements” (Kitsuse and Spector, 1973, p. 418), the criteria chosen by the affected community that describes the social conditions as problematic. By prioritizing the community’s perspective like this, Kitsuse and Spector’s (1973) theory encourages researchers to set aside their own biases and consider the claims of those who are directly experiencing the (putative) social problem.

As a result, social problems can be defined as “the activities of groups making assertions of grievances and claims to organizations, agencies, and institutions about some putative conditions” (Kitsuse and Spector, 1973, p. 146) referred to also as “claims-making” (Kitsuse and Spector, 1973, p. 146). These claims-making activities are “a demand made by one party to another that something be done about some putative condition” (Spector and Kitsuse, 2017, p. 78) and can be studied through rhetoric, “the study of persuasion” (Best, 1987, p. 102). Thus, the purpose of my research’s methodology is to understand how various claims-makers constructed rhetorical demands about the putative social conditions they associated with lawful access legislation.

This chapter begins by establishing the epistemological foundation of my theoretical framework, focusing on its constructionist approach, differing interpretations of social problems, critiques of social problem theory, and contextual elements I have decided to include based on the works of other researchers. It then discusses claims, their components, and how they are used to rhetorically construct social problems.

Epistemological Foundation

As discussed above, social problem theory's epistemological position is that researchers should define social problems according to criteria of those who claim to be affected by them (Kitsuse and Spector, 1973; Kitsuse and Spector, 1975). Because of this, it is a highly useful theoretical framework that can help explain how issues that surround surveillance, such as the balance between security and civil rights (Baker, 2003), risk (Lyon, 2003; Mathiesen, 2013), cybercrime (Akdeniz, 2002; Etter, 2001; Pallasas, 2011), terrorism (Finley and Esposito, 2014; Krebs and Lobasz, 2007; Lyon, 2003; Mathiesen, 2013; Ryan, 2011; Sahill, 2019), and privacy (Andrejevic, 2007; Bailey, 2008; Mathiesen, 2013; Nyst, 2018; Steeves, 2008), are mobilized, defined, and contested by political individuals or groups as they discuss and debate the existence of socially-constructed problems and potentially lead to state decisions as to whether or not surveillance is the appropriate solution to these problems.

Social problem theory arose from critiques of functionalist analyses of social problems which "have tended to regard social problems more or less as Durkheimian social facts⁴ that occur independently of the ways in which they are perceived by members of society" (Weinberg, 2009, p. 61). Accordingly, functionalist scholars generally focused their studies on "social disorganization or deviant behavior" (Kitsuse and Spector, 1973, p. 409). From this perspective, the researcher is responsible for identifying social problems based on "objective" social conditions which they consider to be dysfunctional, and the subjective experiences of the people who live in these conditions cannot be used to study social problems. Instead, the functionalist

⁴ According to Durkheim (1967), social facts are *external* forces that have a coercive effect on the way individuals act, think, and feel. Durkheim (1967) further argues that sociological research must maintain an objective perspective and avoid individual subjectivity – "*On peut poser en principe que les faits sociaux sont d'autant plus susceptibles d'être objectivement représentés qu'ils sont plus complètement dégagés des faits individuels qui les manifestent*" (p. 19) – by observing the behaviours, social structures, and communications that concretely represent "subjective" concepts such as morals and norms rather than relying on individuals' interpretations.

concept of *anomie*, a loss of social norms that occurs “because the relationships between [social] organs are not regulated” (Durkheim, 1984, p. 304) and standards of conduct and activity are no longer clear, can be used by researchers to identify and define social problems according to the researchers’ assessment of normative disruptions that (should) negatively affect people’s lives. Issues that researchers commonly associated with surveillance – such as cybercrime (see Akdeniz, 2002; Etter, 2001; Pallaras, 2011), terrorism (see Lyon, 2003; Mathiesen, 2013), the collaboration between the state and social media companies (see Fuchs and Trottier, 2017; Kelly, 2022), state secrecy (see Nasu, 2015; Nyst, 2018), or the general public’s privacy expectations (see Bailey, 2008; Steeves, 2008) – would be problematized by the functionalist perspective because they disrupt social norms related to law enforcement, safety, private communication, or state accountability in a way that deregulates and denormalizes the longstanding relationship between the citizens and the state, and the citizens’ expectations of acceptable state intervention into their personal lives. This presupposes that the functionalist researcher can objectively define norms and identify the thresholds of anomie. While this may be possible within the theoretical framework, I argue that this cannot be achieved in practice within the context of surveillance studies because of the way “national security” – a core component of pro-surveillance discourse (see Baker, 2003; Nasu, 2015) – is used to present surveillance as a functional social fact for the sake of public safety and justify the disruptions it causes⁵. Any number of privacy measures can potentially be considered disruptive to national security, which is why proponents of national

⁵ More specifically, I argue that a functionalist analysis of state surveillance as a social problem would likely interpret surveillance measures as a form of anomie because they disrupt pre-existing legal norms and privacy rights. However, Neocleous (2006) argues that exceptional emergency or security measures often become normalized over time and, although they may be disruptive initially and potentially create a state of anomie, the general trend is that they will establish new functional norms over time as they become accepted in society. Therefore, the social problem of state surveillance, as a form of anomie, would eventually establish new norms and would no longer be considered a social problem from the functionalist perspective. Because of this, I believe the functionalist perspective on social problems is fundamentally incompatible with my research, which takes a more critical perspective on the normalization of surveillance.

security consider online anonymity (see Akdeniz, 2002; Armstrong and Forde, 2003; Rohret and Kraft, 2011), the Dark Web (see Shillito, 2019), or any features which allow users to avoid surveillance to any extent, problematic. Likewise, any number of national security measures could also be considered potentially disruptive to society, which is why privacy advocates consider issues such as the collaboration between states and telecommunication companies (see Huery and Rosenberg, 2004), the legalization of previously illegal surveillance methods (see Ogasawara, 2022), or the globalization of surveillance (see Nasu, 2015) to be problematic. These potential disruptions have historically been framed within the context of the balance between security and civil rights (see Baker, 2003; Bannister, 2005), which suggests that “reasonable” limits must be placed on civil rights such as privacy in order to implement policies that are deemed necessary to protect national security (see Lyon, 2003; Mathiesen, 2013). However, the very concept of a “balance” implies that the relationship between the social organs of state surveillance and personal privacy *are* functionally regulated by some social norms. It would therefore be difficult, if not impossible, to critically examine lawful access and surveillance as social problems from the functionalist perspective.

In line with this, social problem theory critiques the functionalist perspective’s epistemology on several points. The fundamental critique is that functionalism “has not created a distinctive field but simply assimilated social problems into functional analysis, emphasizing dysfunctions and disorganization” (Kitsuse and Spector, 1975, p. 584). In other words, rather than adapting itself specifically to the study of social problems, functionalism operates on the premise that social problems can be observed, identified, and categorized based solely on their (dys)function within society. The researcher is therefore positioned as the sole arbiter of what is and is not a social problem based on their observation of social facts.

This epistemological position raises two problems that are also subject to theoretical critique. First, the position of functionalism “seems to be that when the sociologists and the members of a society disagree on whether a condition is a substantial discrepancy between expectations and actuality, the sociologists' definition is to be favored” (Kitsuse and Spector, 1973, p. 410). This can potentially create a gap between the researchers’ “objective” external observations and the affected community’s internal subjective experience of social facts or social conditions. From a methodological perspective, such a contradiction would not necessarily be a problem if it is taken into consideration, but the possibility of such a conflict can be avoided entirely by using a different theoretical framework.

Second, in order to study social problems from a functionalist perspective, “the researcher would have to know all of the consequences of a given condition or activity in all sectors of a society [and] show that, overall, these consequences tended to erode or undermine the 'proper' functioning of the society” (Kitsuse and Spector, 1973, p. 409). To accomplish this, a researcher would need to know, with absolute certainty, all the possible consequences of all the possible social conditions and establish clear, objective standards for which conditions are considered most functional within society. This is simply impossible.

Moreover, the underlying epistemological problem is that the functionalist perspective prioritizes outcomes and consequences, which is not the purpose of my research. The focus of my research is on claims-making activities – the rhetorics expressed by various groups and individuals involved in lawful access legislation, how these rhetorics were used to socially construct the putative social conditions of lawful access legislation, and how these putative social conditions were used to construct social problems around lawful access legislation. My interest is

in the various *subjective* interpretations of what lawful access, national security, and privacy should be, and how these interpretations were mobilized in claims-making activities.

To address the functional perspective's epistemological problems, Fuller and Myers (1941a, 1941b) propose the value-conflict approach. The value conflict theorised by Fuller and Myers (1941b) is twofold: first, problematic social conditions are sometimes caused by certain cultural values; second, values can obstruct solutions to social problems when people believe the proposed solutions run counter to their values. Therefore, value-conflict theory considers "both the objective conditions and the subjective awareness of social problems" (Kitsuse and Spector, 1973, p. 412) by studying how "value-judgments lead people to denounce conditions as undesirable and repugnant to them and to define such conditions as social problems" (Kitsuse and Spector, 1973, p. 413). The "objective" observation of the social condition is still an important concern, but a social problem is only recognized if the community considers the condition to be problematic according to its values, introducing a subjective perspective that the functionalist approach lacks.

The value-conflict theory's focus on the way communities respond to social conditions and identify problems based on values that are sometimes contradictory could contribute to the study of Canadian lawful access. The balance between security and privacy is, essentially, a conflict between two different sets of values, and the debates about lawful access reveal the value beliefs and priorities of the groups and individuals involved. Using this perspective, it would be possible to frame the debates as a conflict and examine how a "stable" balance was achieved at the conflict's conclusion.

However, value-conflict theory does not fully disengage itself from the functionalist perspective's pursuit of objectivity, which leaves it open to critique. Kitsuse and Spector (1975)

suggest that the value-conflict approach has been “sensitive to the charge of subjectivism from their critics” (p. 588) and takes objective social conditions into consideration in order to protect itself from these critiques. However, Spector and Kitsuse (1973) further argue that “the attempt to explain both the objective and subjective aspects of social problems deflects the originality and thrust of the value-conflict formulation” (p. 146), which limits its theoretical relevance. Although the inclusion of subjective elements does distinguish value-conflict theory from functionalism and offers some theoretical originality and innovation, value-conflict researchers “did not follow their own bold and provocative beginning to its logical conclusion” (Kitsuse and Spector, 1975, p. 584) and “failed to generate a research tradition or to translate its critique of functionalist formulations into a positive approach to theory and research” (Kitsuse and Spector, 1975, p. 584). By attempting to avoid the critique that it is too subjective, value-conflict leaves itself vulnerable to those critiques that apply to the functionalist perspective: that the opinions of the researchers are more important than those of the affected communities; that there is a potential for discrepancies between the opinions of the researchers and those of the community; and that the researcher requires a complete understanding of the social conditions and their consequences in order to conclude that they are problematic to society. Although the inclusion of value-based subjectivity does mitigate these critiques, a full commitment to prioritizing subjective experience over “objective” conditions is needed.

Social problem theory offers a clear solution to this problem. Spector and Kitsuse (1973) suggest that by using a theoretical perspective based on social constructionism, it is possible to take full advantage of subjective experiences as the focus of research. They argue that a theory of social problems should both offer “[a] definition of the phenomenon, the subject matter for analysis, in a clear and unambiguous manner amenable to empirical investigation” (Kitsuse and

Spector, 1975, p. 408) and “[j]ustify the addition of the new conceptual category 'social problems' by distinguishing its content from that of other previous or related categories” (p. 408). To address these two points, Spector and Kitsuse (1973) propose a four stage natural history model that can explain and examine how social problems are identified and socially constructed.

Stage One of a social problem's development begins “with the collective attempts to remedy a condition that some group perceives and judges offensive and undesirable” (Spector and Kitsuse, 1973, p. 148) and “attempts to transform private troubles into public issues” (p. 148). This is fundamental to my research, which examines how issues such as national security, risk, terrorism, cybercrime, civil rights, and privacy were mobilized in the public sphere by various parties to establish or contest the existence of problems related to lawful access legislation.

To publicize issues, “social problems are raised through the claims⁶ of dissatisfied groups” (Spector and Kitsuse, 1973, pp. 148-149). At this stage, claims can be analyzed according to “the power of the group, the nature of their claims, and the strategies and mechanisms of pressing claim” (Spector and Kitsuse, 1973, p. 149). The power of a group is “conceived as the ability of a group to realize the demands it makes” (Spector and Kitsuse, 1973, p. 149) and “groups that have more membership, greater constituency, more money, greater discipline, and organization will be more effective in pressing their claims than groups that lack these attributes” (Spector and Kitsuse, 1973, p. 149) because they have more resources to mobilize in order to make their claims heard. According to Spector and Kitsuse (1973) the

⁶ Rhetorically, claims are logical conclusions based on grounds that establish the facts of the claim and warrants that justify a response based on the grounds (Toulmin, Rieke and Janik, 1984). In the context of social problem theory, social problems are constructed through claims-making (Spector and Kitsuse, 2017).

effectiveness of a claim is defined by how vague or specific the sense of public dissatisfaction it produces is, and how specifically it assigns responsibility for the social problem:

1. The more vague the sense of dissatisfaction, the more diffuse and general will be the claim, and the less likely will be the recognition or response to the claim; and the less likely will there be a specific remedy enacted.
2. The more vague the sense of dissatisfaction, the less likely is the group able to affix responsibility or propose remedies for their discontent.
3. The less the group is able to affix responsibility for their dissatisfaction, the less able they will be to choose a target to which to direct their complaint.
4. The less the group is able to affix responsibility for their dissatisfaction, the less able they will be to counter the charge that they themselves are to blame. (Spector and Kitsuse, 1973, p. 150)

Because of this, claims that have a clearly-defined scope and that attribute the problem to a specific cause should be the most effective and credible. Finally, claims-makers must evaluate the methods they use to make their claims, specifically “the way that claims are delivered, expressed, or made public” (Spector and Kitsuse, 1973, p. 150) and the process used to “identif[y] the party to whom the complaint should be addressed” (Spector and Kitsuse, 1973, p. 151), in order to ensure they are using a form of communication that is appropriate to their audience and that their audience considers the claims relevant and is capable of acting on them.

Stage Two is the formal recognition of the claims-makers's claims by an official agency relevant to the social problem raised, which “may range from passive acknowledgment of the claim to active attempts to control, regulate, or eliminate the condition at issue in the claim”

(Spector and Kitsuse, 1973, p. 152). The involvement of these official agencies “may lend prestige to the original protest group, but at the same time may begin to overshadow and thus reduce the significance of its activities” (Spector and Kitsuse, 1973, p. 153) or “take over the issue, making it their own, and neutralize or eliminate the original protest group” (Spector and Kitsuse, 1973, p. 153). Thus, while the involvement of an official agency may be necessary in order to secure the resources or legitimacy needed to “solve” a social problem or address problematic putative social conditions, the agency can take over the claims-making activities to reinterpret and reconstruct the original social problem in order to suit its own interests and priorities. In the case of lawful access legislation, this stage would examine how the Canadian government, as the organisation responsible for legislation, received and responded to claims made about security and privacy.

Stage Three “makes a distinction between claims about conditions that characterize social problems activities in Stage One, and claims about the manner in which procedures negotiated in Stage Two function to deal with those imputed conditions” (Spector and Kitsuse, 1973, p. 155) and examines how “assertions about the inadequacy, inefficacy, or injustice of the procedures may themselves become the conditions around which new social problems activities are organized” (Spector and Kitsuse, 1973, p. 155). This focus of this stage is not on the initial social problem, but on the official agency's reaction to and handling of the problem, especially when some claims-makers who may or may not be related to the initial claims are unsatisfied with the official agency's response and seek to construct it as a new social problem, which may result in “a renegotiation of procedures, reform of existing practices, dismissal of a high level administrator, possibly the establishment of a new, more specialized agency” (Spector and Kitsuse, 1973, p. 156) or “generate an atmosphere of fundamental distrust of institutionalized

procedures, an attitude of cynicism, resignation, and despair, and a lack of confidence in established institutions” (Spector and Kitsuse, 1973, p. 156) depending on the effectiveness and outcome of the new claims-making activities per Stage One and Stage Two. Thus, Stage Three would focus on the way involved parties responded to the Canadian government’s handling of lawful access legislation by resolving issues such as the balance between security and privacy.

Finally, Stage Four is the point where complainants' “focus shifts from complaints and protests against established procedures to creating and developing alternative solutions for their perceived problems” (Spector and Kitsuse, 1973, p. 156) though activities that are “organized by claims that challenge the *legitimacy* of established institutions and the procedures they organize for the processing of claims” (Spector and Kitsuse, 1973, p. 156, emphasis in original) instead of continuing to rely on official agencies. This stage can result in either “the creation of alternative institutions as a means of developing a social and political base for radically changing the existing procedures or (2) disaffiliation and withdrawal from the institutional system to create alternative institutions as limited solutions for group members” (Spector and Kitsuse, 1973, pp. 156-157). If their claims about problematic social conditions are not addressed, claims-makers have no recourse but to create new solutions themselves. Since my research focuses specifically on legislation and does not include the consequences of lawful access legislation after it was implemented, this step is not relevant to my research and was not part of my analysis, but it should still be mentioned since it is part of the four stage model.

This model’s focus on subjective claims offers a concrete topic for empirical research and clearly defines how social problems may be categorized based on these claims. This approach completely rejects the study of objective social conditions on the grounds that it “misdirects our attention, implying that objective and recurrent properties are of analytic consequence or interest

(to social constructionism) and leads us away from the flux and emergent forms of social problems discourse” (Ibarra and Kitsuse, 2003, p. 23). Instead, social problem theory defines social problems based on claims-making activities (see Spector and Kitsuse, 2017), more specifically as “the activities of those who assert the existence of conditions and define them as problematic” (Spector and Kitsuse, 2017, p. 74) and “[t]he activity of making claims, complaints, or demands for change” (Spector and Kitsuse, 2017, p. 74). As such, social problem theory identifies problems not according to the researcher’s observations and “objective” assessment of social conditions and of their consequences on affected communities, but according to the empirical observation of claims-making activities and of claims made about social conditions⁷.

Weak Readings of Social Problem Theory

Although social problem theory was originally developed at least in part as a response to value-conflict theory’s unwillingness to fully reject the researcher’s objectivity, some variations of it have attempted to include objective observation while attempting to maintain a constructionist perspective. As a result, social problem theory “is subject to both weak and strong interpretations” (Best, 2003a, p. 51), and while my research adheres to a strong interpretation of the theory, weaker interpretations raise points and critiques that must be discussed in order to clarify and defend my epistemological position.

Weak Readings Based on the Integration of Subjective and Objective Social Conditions

Some social problem researchers have “proposed integrating [objective and subjective] perspectives, borrowing insights from each other to develop a more complete interpretive

⁷ The social conditions described by the claims can be putative conditions or objective conditions. However, within social problem theory, social conditions are relevant as data because of the way they are part of (and produced by) claims-making activities. The factual reality of the social conditions is a separate from the social conditions as they are described by the claim.

framework” (Best, 2003a, p. 56) which includes both the objective conditions and the subjective experience of social problems, a perspective that differentiates itself from value-conflict theory mostly because it does not necessarily associate social problems with value-based conflicts between individuals or groups. As Best (2003b) explains, “sociologists examining social problems construction found it tempting to study moral panics and drug scares, alarms raised over fanciful or at least exaggerated dangers” (Best, 2003b, p. 137). Doing so allowed them to examine the factual “gap” between socially constructed putative social conditions produced through claims-making and directly observable objective social conditions. However, studying subjective claims and observable social conditions together like this leaves researchers vulnerable to the same critiques that were levied against the functionalist theory or value-conflict theory: that the criteria used to identify social problems do not necessarily reflect the subjective experiences of the people who are directly affected by the social conditions, or that the theory attempts to study subjective experience without making a firm theoretical commitment to doing so. Best (2003b) describes one example of this as “*vulgar constructionism*” (p. 137, emphasis in original), an interpretation that is used to dismiss the existence of social problems entirely by arguing that since there is no empirical evidence that a problem exists, then it is only an imaginary social construct and there is no need to expend resources to address it. Studying social problems like this can be scientifically interesting because it problematizes the contradictions between claims-makers’ putative statements of fact and the researcher’s observation of the facts, but, as mentioned previously, the focus of my research is on the claims-making process used to construct social problems around lawful access, not on the consequences of lawful access. Comparing the claims made about the effects of lawful access while the legislation was being

developed to the effects of the legislation after it was implemented is beyond the scope of my research.

In social problem theory, claims, not social conditions, are the object and subject of research. From a theoretical and analytical perspective, “objective” social conditions are irrelevant because they are non-data beyond the claims that are made about them. Attempts to combine objectivist and constructionist theories have accordingly led to accusations of “[ontological] gerrymandering [in which] one privileges one symbolic rendering of a particular condition as objectively superior to other renderings in order to first distinguish the condition from people’s symbolic experiences and activities regarding it and, then, ultimately, to defend a systematically anti-objectivist theoretical program” (Weinberg, 2009, p. 65), as it allows “objective” empirical observations to legitimize or delegitimize the claims made about social conditions in an attempt to distinguish between “true” and “false” social problems. However, the assessment of a claim’s validity is itself a subjective opinion that can be influenced by researcher bias. As Best (2003a) argues, researchers are likely to make “less explicit assumptions about objective conditions, assumptions that frame the research agenda” (p. 59). The *choice* to study the claims made about any given social problem is inevitably related to the researcher’s personal interest in the topic, and at the very least *suggests* that the researcher possesses some sort of bias, such as the belief that a social problem does exist, even before they have had the opportunity to collect and analyze data.

To address these potential biases, researchers “must renounce the scientific myth of wholly detached and disinterested inquiry, and acknowledge that neither we as researchers nor those we study can ever intelligibly leave the domain of embodied, invested, and fully purposeful practical action” (Weinberg, 2009, p. 69), acknowledging how they position themselves in relation to the

claims they are studying *and* in relation to the putative social conditions that are constructed by these claims. By doing this, social problem researchers could clarify their object of study – the claims-making activities – while acknowledging personal interests that could bias their decisions related to sampling, data analysis, or any other part of the research process. This would make it easier to critically evaluate the research and ensure that it accurately represents the claims-makers' positions. Nevertheless, this is a problem that only exists when relying on weak readings of social problem theory, and it can be avoided entirely by eschewing weak readings and focusing on the core theoretical foundation of social problem theory.

The weak readings of social constructionism described above are based on a scientific interest in objective social conditions, either to find practical solutions to social problems or to better understand “excessive” reactions to relatively minor social problems. These perspectives attempt to achieve their goals by seeking a compromise between positivist and constructionist approaches, only to undermine social problem theory's fundamental premise that social problems are constructed through claims-making activities, which creates an irreconcilable theoretical contradiction within the context of social problem theory.

Weak Readings Based on Critiques

Other weak interpretations of social problem theory stem from critiques of the theory. One such interpretation, argued by Bockman (1991), states that social problem theory is “a theory of claims-making devoid of meanings, intentionality, and motives” (p. 453) because it focuses only on the claims themselves and ignores the circumstances of the claims-makers and the motivation behind the claims, which should also be included in the analysis.

In response to this critique, I argue that, as the main focus of social constructionism is to understand how social problems are constructed through claims, the claims-makers' intentions or motives are not necessary to the study of social problems; they are simply a different topic, much like objective social conditions which do not need to be taken into consideration because they are not the subject of social problem theory. As Bogard (2003) explains, “[s]trict constructionists prefer to focus on *how* questions” (p. 210), which are core questions of the four stage model of social problems: how complainants use claims to construct social problems; how the social problems are communicated to institutions and to the public; how the responsibility for putative social conditions is assigned; how institutions react to the claims; how complainants react to the institutions' reactions; and so on. Moreover, while social problem theory cannot easily analyze the hidden or the implied meanings, intentions, or motives of claims-makers, one motive will always be self-evident: to make claims about the putative existence of problematic social conditions in order to address them. This intention is simply integral to the claims-making process.

Another critique is proposed by Best (2003a), who argues that “constructionists inevitably adopt an epistemologically inconsistent position” (p. 56) as they attempt – and fail – to focus on the construction of social problems without paying attention to the context of the problem. This critique requires greater consideration. As Weinberg (2009) states, “all activities concerning putatively problematic conditions are embedded in historical, cultural, and interactional contexts that are themselves empirically discoverable, available, and, I would argue, absolutely indispensable, for use both by members and by ourselves (in our own distinctly sociological efforts) to better understand those activities” (p. 67), so it is difficult, if not impossible, to study a claim made about social problems without going outside the claim itself to examine its context;

lawful access legislation in particular exists within a broader technological, legal, and political context that cannot be ignored.

As a result of this critique, social constructionists “are left to contend with the issue of how to deal with the issue of how to deal with context without betraying the fundamental commitment to the perspective” (Holstein and Gubrium, 2013, p. 189). The point of this critique is that social constructionism should recognize that “objectivity is simply a matter of answering questions in ways that account for the available evidence pertaining to those questions better than anyone else” (Weinberg, 2009, p. 74) in order to pursue a more complete study of social problems, which could include studying the links between claims and broader social trends in order to understand their history and possible implications.

This critique is difficult to refute because it raises a valid point about the importance understanding claims within their social context, but doesn’t necessarily interfere with the analysis of social problems themselves. Therefore, I argue it is possible to situate claims-making activities within a broader context while maintaining a strong reading of social problem theory by introducing the context into the analysis of the claims without using it to make judgments about the validity or factuality of the social problem.

Contextual Constructionism

Although my research utilizes a strong reading of social problem theory based on strict social constructionism, I borrow elements of contextual constructionism, a concept used by Best (1987, 2003a, 2003b). Best (2003a) argues that social constructionism must “study claims-making within its context of culture and social structure” (p. 61) and that “[a] strong reading [of social problem theory] that ‘never leaves language’ is an illusion because language never leaves

society” (p. 63). Therefore, the language used to engage in claims-making activities and construct social problems such as surveillance is influenced by society: societal norms, societal expectations, societal priorities, etc. Additionally, due to the fact that “the very reality of social problems depends on the ways they are perceived and managed by members of historically and culturally specific constituencies” (Weinberg, 2009, p. 61), it is necessary to acknowledge that while social problems are constructed by the literal language of a claim, the social context of the claim, such as the way the putative social conditions are framed as problematic, the groups voicing the claims, the groups targeted by the claims, the means used to assign blame for the problem, and the means used to attract support for the claims, are important. In fact, these contextual elements are part of the four stage model and are used to analyze the claims-making activities – without making any statements about objective social conditions or the validity of the claims. Thus, while Best (2003b) argues that “[s]cience is a social construction; but it is grounded in and shaped by scientists' experiences with the empirical world” (p. 141), I counterargue that, within social problem theory, scientists' experiences could and should be used to situate claims within broader historical trends and identify patterns without including any discussion of “objective” social conditions.

Reconciling a Strong Reading with Contextual Constructionism

To maintain epistemological and theoretical consistency with social problem theory while drawing on elements of contextual constructionism, I argue that the inclusion of social context should focus on two elements of social problem theory: first, that “the 'subjective elements' of social problems [...] is (*sic*) the distinctive subject matter of the sociology of social problems” (Spector and Kitsuse, 1973, p. 146); and that the purpose social context's inclusion is “to account for the *emergence and maintenance of claim-making and responding activities*” (Kitsuse and

Spector, 1973, p. 415, emphasis in original). The first condition ensures that the analysis remains focused on the claims-makers' subjective experiences, while the second condition ensures that the inclusion of social context contributes to social problem theory's objectives and is useful to the analysis.

Bogard (2003) offers a similar approach by using interpretative context – the way conditions and claims are interpreted – and environmental context – material conditions and relationships between claims-makers or social groups – to inform the analysis of claims-making activities and understand why certain claims were made and why, or how and why they were communicated to a specific audience. To avoid the problems associated with ontological gerrymandering, the inclusion of context should, per Holstein and Gubrium's (2013) recommendation, accurately represent the claims-makers' construction of their social or material reality. This would maintain a strong reading of social problem theory even if the broader context is taken into consideration.

The Components of Claims

The four stage history model examines how claims-making activities develop and produce social problems over time, but it acts on a broader scale and focuses more on the interactions between claims-makers. If social problems are produced by claims and claims-making activities, it is necessary to understand what claims are and how they are constructed in order to apply social problem theory. According to Toulmin, Rieke and Janik (1984), claims can be defined as “some ‘destination’ which we may arrive at for ourselves as a discovery, or else may be invited to arrive at by somebody else, as an assertion; and the first step in analyzing and criticizing the argument is to understand the precise character of that destination” (p. 25). More concretely, claims are “assertions put forward publicly for general acceptance” (Toulmin, Rieke and Janik, 1984, p. 29) based on their internal logic; though they may not succeed, claims are

formed with the intent to convince someone that a given course of action is correct. The “journey” to this rhetorical destination can be divided into three components: the grounds, the warrant, and the backing.

Grounds are “statements specifying particular facts about a situation” (Toulmin, Rieke and Janik, 1984, p. 37) which are used to “establish *truth, correctness, or soundness*” (Toulmin, Rieke and Janik, 1984, p. 38). The grounds used to establish a claim vary according to “the nature of the enterprise concerned and on the particular contexts of the arguments themselves” (Toulmin, Rieke and Janik, 1984, p. 41) and they are used to “provide the basic facts which serve as the foundation for the discussion which follows” (Best, 1987, p. 104). In the context of social constructionism and social problem theory, the grounds should be considered statements of putative facts that establish the accepted premise of a claim rather than a statement of “real” or “objective” fact.

By establishing the facts, grounds establish the domain and orientation of a social problem. A domain statement “identifies a phenomenon, setting its boundaries or domain” (Best, 1987, p. 104), which establishes what is and is not part of the phenomenon. An orientation statement provides “some assessment of the sort of problem it is” (Best, 1987, p. 105) and of the field of expertise that should be called upon to seek remedial measures. Thus, the domain statement provides a definition of the social problem and the orientation statement points to the desired solution.⁸

⁸ As discussed in chapter 2, security risks are often used to justify new surveillance measures. In this general context, the domain statements define the security risk and the orientation statements present surveillance as the necessary solution.

Additionally, the grounds can be used to establish common ground between two claims-makers and determine “what things they are both prepared to accept as not needing to be questioned or established” (Toulmin, Rieke and Janik, 1984, p. 38). The common ground – or lack thereof – determines what the claims-makers will communicate about when they assert and debate the value of claims and the existence of social problems. Even if there is no common ground, the grounds of the claim can still be used to understand how claims are made as a result of specific circumstances, or how the grounds put forward by similar claims vary over time. In any case, the first stage of social problem construction begins when a claims-maker produces facts about the existence of problematic social conditions.

Warrants are “statements indicating how the facts on which we agree *are connected to* the claim or conclusion now being offered” (Toulmin, Rieke and Janik, 1984, p. 45, emphasis in original). Warrants are used to “justify drawing conclusions from the grounds” (Best, 1987, p. 108), providing a logical link between the grounds and the claims and, in the case of social problems, creating an obligation to acknowledge that the social conditions described in the grounds are problematic and that they must be addressed somehow. Within the rhetoric, “references to warrants may be oblique or implicit” (Best, 1987, p. 109), so identifying the warrants used in a claim relies on the researcher’s subjective interpretation.

Finally, the backing is “the body of experience relied on to establish the trustworthiness of the ways of arguing applied in any particular case” (Toulmin, Rieke and Janik, 1984, p. 61), emphasizing the credibility and authority of the claims-maker rather than the claim itself. Although backing is important to the persuasiveness of a claim, I am most interested in mapping out the meanings ascribed to lawful access as a social problem. Accordingly, backing takes a secondary role in my research, which primarily focuses on the internal logic of the claims – the

links between the grounds, warrants, and claims used to make assertions about privacy, surveillance, and lawful access – rather than “external” factors such as the credibility of the claims-maker. Because of this, my analysis is based on the rhetorical model of Best (1987), who examined grounds, warrants, and claims/conclusions⁹. In the context of social problem theory, the grounds are the putative “facts” used by claims-makers to describe social conditions, the warrants justify the existence of a social problem, and the conclusion asserts the existence of a social problem. As indicated below, claims-makers are able to rhetorically construct social problems through this process. By unpacking it in the context of lawful access, my project seeks to better understand the social meanings that have emerged to define the issues and the possible solutions.

Condition-Categories

At their most fundamental level, claims combine grounds, a warrant, and a conclusion to produce persuasive assertions, but the claims used to construct social problems possess other dimensions. According to Ibarra and Kitsuse (1993), rhetorical claims-making expresses condition-categories, which can be defined as “typifications of socially circumscribed activities and processes – the ‘society’s’ classifications of its own contents – used in practical contexts to generate meaningful descriptions and evaluations of social reality” (p. 26) and as “the terms used by members to propose what the social problem is ‘about’” (p. 26). The concept of “condition-categories” is important because it “alerts us [researchers] to attend to the ways in which the denotations and connotations of the term become the subject of a kind of articulation contest on

⁹ Best (1987)’s use of the term “conclusion” is meant to clearly differentiate between the use of “claim” in the constructionist sense (i.e., claims-making activities or assertions containing the grounds, warrants, and claims) and the use of “claim” as a logical conclusion based on the grounds and warrants. Likewise, my research uses the term “claim” to refer to the totality of the rhetorical assertion containing the grounds, warrants, and conclusion, and “conclusion” to refer specifically to the figurative “destination” of the rhetoric based on the grounds and warrants.

the part of members to establish what the social problem is ‘really about’” (Ibarra and Kitsuse, 1993, p. 27) and draws attention to the symbolic meaning of the claims rather than its strict literal meaning, which makes it possible to extend the (comparatively) narrow issue of lawful access into a broader trend of claims related to privacy and surveillance in general. This in turn potentially allows results to be generalized to other claims-making activities that are “about” similar putative social conditions and social problems.

The importance of symbolism is also seen in the fact that “claims-making activities reflect substantive concerns on the part of participants, but analytically [researchers] take those claims to be reflective of the interplay between [claims-makers’] moral sensibilities and the dynamics of the process itself” (Ibarra and Kitsuse, 1993, p. 28), so that the framing of a claim reflects the moral beliefs of the claims-makers, not merely their assessment of social conditions. In contrast, “[t]he term *social conditions*, with its connotations of objective and recurrent properties, misdirects our attention, leading us to miss the central question of how there can be social problems discourse in the first place” (Ibarra and Kitsuse, 1993, p. 28), and would therefore overlook the affected group’s moral sensibilities, which would not be represented by “objective” social conditions. This allows the term “condition-categories” to better support the social constructionist perspective of social problem theory and emphasizes that the putative social conditions that surround lawful access are, within the context of my methodology, produced by claims-making activities, including claims-makers’ assessments and categorization of their conditions.

According to Ibarra and Kitsuse (1993), rhetoric is a key concept of social problem theory because it encompasses “the constitutive techniques and processes that are entailed in claims-making as such” (p. 30) and that are used to communicate – and therefore construct – the

existence of a social problem based on putative conditions. This rhetorical process can be examined through four dimensions: “rhetorical idioms, counterrhetorics, motifs, and claims-making styles” (Ibarra and Kitsuse, 1993, p. 30). Each dimension provides a different way to focus attention on a social problem.

Rhetorical Idioms

Rhetorical idioms¹⁰ are defined as “definitional complexes, utilizing language that situates condition-categories in moral universes” (Ibarra and Kitsuse, 1993, p. 30), drawing attention to the moral symbolism of the claim and of the condition-categories it expresses. The subjective moral element of the idiom represents *why* the claims-makers believe the condition-categories constitute a social problem.

The first idiom, the rhetoric of loss, “is not concerned with mourning the extinction of something but rather inveighing against its devaluation” (Ibarra and Kitsuse, 1993, p. 33). It focuses on the reduction, diminishment, or decay of some object over time, claiming that “[i]t is by virtue of the loss of prestige or value accorded to the sacred object that its existence is threatened” (Ibarra and Kitsuse, 1993, p. 33), and “[t]he concept of *protection* assumes a central position in this rhetorical idiom's remedial discourse” (Ibarra and Kitsuse, 1993, p. 33) to prevent further loss. The moral principle of this idiom is that the devaluation of the “sacred object” is a loss for society as a whole, and that the loss must therefore be prevented.

A second rhetorical idiom, the rhetoric of entitlement, “emphasizes the virtue of securing for all persons equal institutional access as well as the unhampered freedom to exercise choice of

¹⁰ All the rhetorical idioms defined by Ibarra and Kitsuse (1993) are listed in this section because they were all considered during coding. The rhetorical idioms that were found to be most relevant to the analysis of the data are defined more specifically in the Coding section.

self-expression” (Ibarra and Kitsuse, 1993, p. 34) in order to prevent discrimination and promote egalitarianism. In this rhetoric, “[t]he concept of *expansion* is central to this idiom’s remedial vocabulary” (Ibarra and Kitsuse, 1993, p. 34, emphasis in original), and it therefore drives the claims to expand the scope of the entitlement, institutional access, and freedom of self-expression for the betterment of society. Within this idiom, putative social conditions would be considered problematic if they restrict freedom or prevent access to social institutions.

The rhetoric of endangerment is based on condition-categories that “pose intolerable risks to one’s health or safety” (Ibarra and Kitsuse, 1993, p. 35), which produces a rhetoric that “evokes the possibility that the transitory status of the person might be extended and the fear that it is being further curtailed” (Ibarra and Kitsuse, 1993, p. 35). In the “extension,” the health and safety of life are preserved and protected from the endangerment, but when it is curtailed, it faces threats – as defined by putative social conditions – that require urgent intervention according to the claims-makers. In comparison, the rhetoric of loss focuses primarily on the “image of transitory yet custodial human beings entrusted with an irreplaceable legacy” (Ibarra and Kitsuse, 1993, p. 35) and claims that an element of the past is devalued in the present. The idiom of endangerment rather claims that present social conditions create threats for the continuation of the future.

A fourth rhetorical idiom, the rhetoric of unreason, “posits an idealized relationship between the self and the state of knowing, and then locates an instance where that proper relationship is being distorted, undermined, and even destroyed” (Ibarra and Kitsuse, 1993, p. 36) to claim that the targeted behaviour is fundamentally irrational and problematic. This rhetoric is based on the assumption that “in the absence of the pernicious influence, the combined force of being fully informed and in complete control of one’s cognitive powers would result in

preferable courses of action” (Ibarra and Kitsuse, 1993, p. 36) and lead to “better” outcomes. The moral imperative here is that problem-solving decisions should be based on reason and factual information or else they are unsound and create problematic putative conditions.

The rhetoric of calamity is “composed of metaphors and reasoning practices that evoke the unimaginability of utter disaster” (Ibarra and Kitsuse, 1993, p. 37) and is often used to “recognize the existence of other claims-making activities directed at nominally unrelated condition-categories, yet cast things into perspective by demonstrating how those other moral objects are contingent upon the existence of ‘their’ condition-category” (Ibarra and Kitsuse, 1993, p. 37), thereby associating their claims-making activities and social problems to those of other claims-makers in order to establish common grounds and seek rhetorical support for their own claims.

Rhetorical Motifs

Rhetorical motifs are “recurrent thematic elements and figures of speech that encapsulate or highlight some aspect of a social problem” (Ibarra and Kitsuse, 1993, p. 43) and that create a “generic vocabulary conventionally used in claims-making, each term or phrase acquiring distinctive connotations in being situated in one kind of context instead of another” (Ibarra and Kitsuse, 1993, p. 43). The symbolism of the motifs and their ability to communicate claims in the common vernacular allows researcher to study “how the terms of social problems discourse evolve and are fine-tuned, and how their symbolic implications are contained” (Ibarra and Kitsuse, 1993, p. 44), which makes it possible to study how claims-making activities evolve over time and what norms or values they express beyond the literal text of the claim.

The concept of motifs has proven to be critical to my methodology in two ways. First, it helps to elucidate the meaning of rhetorical warrants. Since warrants are often implied, it can be difficult to codify their meaning. However, the motifs used to communicate the warrant contain symbolic language that refers to moral values or norms, and these can be interpreted, albeit subjectively, in order to clearly codify the warrant.

Second, motifs provide analytical support to my decision to draw from Bogard (2003) and include context in my research. In this instance, the motifs provide a window into the context. The motifs expressed by claims-makers represent information – rhetorical grounds or warrants – that they consider relevant to the social construction lawful access. Context is included not by a researcher who wishes to critique the validity of claims, but by claims-maker who draw upon different issues in order to establish their own claims. Rather than examine “objective” social conditions to find empirical data to support or refute the claims made about lawful access, my research compares the motifs found my primary data – the claims-making activities surrounding lawful access legislation – and motifs identified in secondary data pertaining to lawful access, privacy, security, policing, and other relevant issues. This allows me to show if and how the rhetorical claims changed over time and to situate my findings within a broader historical and global context.

Counterrhetorics

Counterrhetorics are defined as “discursive strategies for countering characterizations made by claimants” (Ibarra and Kitsuse, 1993, p. 30) that are aimed at the “claimant's description, proposed remedies, or something other than the candidate problem” (Ibarra and Kitsuse, 1993, p. 31) and seek to “block either the attempted characterization of the condition-category or the call

to action, or both” (Ibarra and Kitsuse, 1993, p. 38) in order to refute the opposing claims-making activities or their necessity. Counterrhetorics can be divided into two categories:

The strategies fall into two classes: (1) sympathetic counterrhetorics, which accept, in part or whole, the problematic status of the condition-category, but which in effect block the request for remedial activities; and (2) unsympathetic counterrhetorics, which countenance neither the proposed characterization and evaluation nor the suggested remedies. (Ibarra and Kitsuse, 1993, p. 38)

Thus, sympathetic counterrhetorics general seek to negate a claim by acknowledging the existence of a putative social problem, but denying demands for a solution. This gives the impression, whether true or not, that the claims-maker cares about the social problem, but delays a solution. Conversely, unsympathetic strategies deny the existence of a social problem altogether.

Counterrhetorics are touched upon briefly here because they are part of social problem theory and need to be addressed, if only for context. However, they were not part of the data coding.¹¹ Though they are an important part of the claims-making process and of the natural history model of social problems, counterrhetorics examine claims as responses to other claims and would have been secondary to my research. In addition, including counterrhetorics to the coding would have added an unnecessary layer of complexity, as each statement would have had to be considered in relation to all other claims to determine whether or not it should be considered part of a counterrhetoric. It quickly became evident during coding that rhetorical motifs and idioms would be sufficient to code the data.

¹¹ Counterrhetorics are discussed in Chapter 3 and Chapter 5 to support specific elements of the analysis in those chapters.

Claims-making Styles

Ibarra and Kitsuse (1993) “introduce the concept of *claims-making styles* in order to suggest a research agenda derived from the central premise of social constructionism — the constitutive character of claims-making activities” (p. 45) and clearly emphasize that *claims-making activities* as a whole should be the subject of social problem theory; the literal context of the claim, while certainly important, does not constitute the entire process. Within social problem theory, the term “style” serves multiple functions and perspectives; used as a noun, it draws attention to “how various groupings of the claimant's bearing, tenor, sensibility, and membership category can inform both a claim's general appearance and specific content as well as instruct auditors on how the claim should be interpreted” (Ibarra and Kitsuse, 1993, p. 45), while when used as a verb, it “refers to the act of fashioning a claim that is consistent with the conventions of claims-making styles, as when one styles, say, a scientific claim” (Ibarra and Kitsuse, 1993, p. 45). In both cases, it is used to describe how a claim is constructed by the claimants and then communicated to its intended audience. Demeanour, tone, verbiage, medium, and other factors used to convey the claim are part of the claims-making process and reflect the claimant's position and their attitude towards the condition-categories and the claim's audience. Thus, claims-making styles serve as “general ways of articulating moral stances” (Ibarra and Kitsuse, 1993, p. 46) and are “as valuable in rendering condition-categories problematic as in making the categories seem unobjectionable, harmless, or otherwise not warranting attention” (Ibarra and Kitsuse, 1993, p. 46). The rhetorical presentation of the claim – or the counterclaim – is part of the claim's construction and part of the way the claim constructs condition-categories and moral realities.

Unlike rhetorical idioms, rhetorical motifs, and counter-rhetorics, claims-making style were not a prominent part of my coding and analysis. Rhetorical idioms and counter-rhetorics are clearly defined and rhetorical motifs can be clearly identified by the recurring use of key terms, but analyzing claims-making styles would require a more subjective interpretation of the data that is not always possible through text. Although some of the claims found in the data had a more obvious tone,¹² accurately gauging every single instance of tone solely from text would not have been practical. Moreover, due to the relatively limited nature of the data, which, as discussed in the following section, focused on parliamentary records, government records, and news articles, the content of the claims was a more important point of analysis than the means used to publish and communicate the claims to their intended audience(s). Thus, excluding claims-making styles from the analysis allowed for greater focus on how different claims-makers rhetorically constructed the social problems associated with lawful access legislation and emphasized the putative social conditions claims-makers sought to define.

Research Methods

Data Collection

Data collection focused on three areas: newspaper articles, public parliamentary records, and documents obtained from the Privacy Commissioner of Canada and the Department of Justice Canada through an access to information request. This was meant to provide a comprehensive overview of the claims made about the lawful access legislation debated between 2009 and 2014.

¹² See pp. 147-160, which discuss the role of political partisanship within the rhetoric and includes statements that clearly convey political outrage.

Newspaper articles were obtained through the *ProQuest Canadian Major Dailies* database (ProQuest, n.d.), using the numbering of the bills as search terms: “Bill C-74,” “Bill C-46,” “Bill C-47,” “Bill C-50,” “Bill C-51,” “Bill C-52,” “Bill C-30,” “Bill C-13.” To prevent confusion with other bills, the searches were restricted to the duration of the relevant sessions of Parliament.¹³ French newspaper articles were obtained through the *ProQuest* database (ProQuest, 2018), using the following keywords: “C-74”, “C-46”, “C-47”, “C-50”, “C-51”, “C-52”, “C-30”, “C-13.” These searches were also limited to the timeframe of the relevant sessions of Parliament and were limited to French language documents. To ensure no news coverage had been missed, I also ran a search using the terms “lawful access” and “accès legal” for articles published between 2002 and 2015. These searches produced 582 relevant newspaper articles, 556 in English and 26 in French¹⁴.

In addition, I obtained House of Commons and Senate records from the website of the Parliament of Canada. These records included the texts of the bills and records of readings, debates, votes, and committee meetings in both the House of Commons and the Senate. In total, there were 80 such documents.

Finally, I used Access to Information to request additional documents about Bill C-30 from the Office of the Privacy Commissioner of Canada and from the Department of Justice Canada. The data showed that news interest in lawful access increased significantly after that bill, so I considered it a critical case, an example of “strategic importance in relation to the

¹³ October 4, 2004 to November 29, 2005 for Bill C-74; January 26, 2009 to December 30, 2009 for Bill C-46 and Bill C-47; March 3, 2010 to March 26, 2011 for Bill C-50, Bill C-51, and Bill C-52; June 2, 2011 to September 13, 2013 for Bill C-30; October 16, 2013 to August 2, 2015 for Bill C-13.

¹⁴ The newspaper articles were originally intended to provide a measure of public opinion about lawful access legislation to see if and how it had changed over time. However, the overwhelming majority articles were written during or after Bill C-30, providing little data. As a result, the focus of the analysis changed to parliamentary records, which, while limited in perspective, provided a much broader timeline.

general problem” (Flyvbjerg, 2001), and I believed that information on that specific bill could help me better understand how lawful access legislation changed over the years. I received 941 pages of documents from the Office of the Privacy Commissioner and 2,670 pages of documents from the Department of Justice Canada.

Coding

Once all the documents were obtained, I read them and organized extracts and quotations according to the claimant responsible for them. Documents were attributed to their stated author. If a document cited someone other than the author, the citation was separated from the rest of the text and attributed to the quoted party. Documents that contained multiple other documents, such as the files obtained through access to information and the documents containing newspaper articles, were separated into their component texts for coding purposes. All documents were given unique identifiers which were added to the excerpt so that the origin of a quote could be easily identified, found, and verified. Texts, statements, and quotes that did not have any applicability to lawful access or to a topic that the broader document was relating to lawful access in some way were deemed irrelevant and excluded from the data. Only the sections relevant to lawful access or to an issue related to lawful access were deemed relevant.

While the quotes were being organized and coded by claims-makers, the claims-makers themselves were simultaneously organized and grouped according to their membership category, an aspect of claims-making style that remained obvious in my text-based data. The goal of categorizing claims-makers according in this manner was to determine if formal organizations or individuals who shared a similar background made similar claims and if or how these claims changed over time. This was most important in the case of the federal political parties of Canada, who were directly responsible for lawful access legislation.

In total thirteen membership categories were identified: Bloc Québécois, civil society, Conservative Party, experts, government, Green Party, industry, journalists, Liberal Party, New Democratic Party (NDP), other, police, and privacy commissioners. Claimants were assigned to the Bloc Québécois, Conservative Party, Green Party, Liberal Party, or New Democratic Party based on their party affiliation in the House of Commons or the Senate of Canada. The civil society category included individuals who spoke on behalf of an organization that did not belong to any other category; the experts category included lawyers who were not associated with an organization that belonged to another category; the government category included all government employees who were not part of the House of Commons or the Senate of Canada; the industry category included all individuals who worked in the telecommunications or technology industry; police included individuals on explicitly spoke on behalf of a law enforcement agency; privacy commissioners included all individuals who spoke on behalf of any privacy commissioner in Canada, either federal or provincial. Journalists included all individuals who wrote newspaper articles and who did not belong to another category¹⁵, but excluded individuals whose articles were specifically identified as letters to the editor or as articles written by members of the general public who wanted to express and publish their opinions. All remaining claims-makers were placed in the “other” category.

After this stage, claims and statements were coded as either “for” or “against” lawful access legislation. This was done primarily for practical reasons to organize the claims in a more manageable manner and to develop a general idea of the different claims-makers and their position. Claims and statements that explicitly supported lawful access legislation, regardless of

¹⁵ There were several cases of experts, police representatives, or privacy commissioners writing newspaper articles to communicate their claims.

any conditions attached to this support, were coded as “for.” Claims and statements that explicitly opposed the lawful access legislation or argued that it should be delayed or altered were coded as “against.” Statements that did not take an explicit position were coded based on their implicit presentation of lawful access or of related topics. If the information or arguments contained within the statements framed lawful access in a positive manner, it was coded as “for.” Statements that framed lawful access in a negative manner were coded as “against.” I made these decisions based on my subjective interpretation of the statements and their contents, but this subjective interpretation was informed by the contents of the more explicit claims of support and opposition. Implicit statements and purely factual statements contained grounds about lawful access, so I associated them with similar grounds found in claims that took a clear position. My rationale was that while they did not take a clear position for or against lawful access, they still indirectly participated in claims-making activities by communicating grounds that were mobilized by clearer, more direct claims. Thus, these implicit statements supported claims by spreading awareness of their grounds, and could be coded as “for” or “against” lawful access legislation despite not taking a clear position themselves.¹⁶

Following this, the individual claims-makers’ statements were coded into three categories: grounds, warrants, and conclusions. Grounds included all statements of fact about putative social conditions and all statements that were meant to provide putative factual information relevant to lawful access or to the claimants’ claims about lawful access. These were the easiest to code, as they contained obvious descriptive statements. Statements were coded as warrants when they evoked some principle – legal, moral, or otherwise – to justify the claimants’

¹⁶ At this point, themes were beginning to emerge from the data: technology, privacy, surveillance, crime, children, and partisan politics. However, they were not operationally defined at this stage, since the primary goal was to gain a general understanding of the data. This took place later during motif-based coding, and statements were re-assigned to different categories at that stage if necessary.

position. Since warrants were often implicit rather than explicit, they were the most difficult and most subjective to code. Finally, statements were coded as conclusions when they prescribed a course of action or argued that pre-established putative conditions should be interpreted or viewed in a certain way; rather than establishing facts to support a claim as grounds do, the conclusion makes a value judgment about social conditions or their consequences based on the facts. In cases where the distinction between grounds, warrants, and conclusions were unclear, often due to the implications of a statement, I categorized the statement according to my best subjective judgment based on the definitions provided above. At the end of this process, the grounds, warrants, and conclusions were aggregated according to category membership.

This process separated the claims into their individual components in order to facilitate the analysis of grounds, warrants, and conclusions. The original document of each statement was still indicated in order to verify statements or their context if necessary, but the following parts of the analysis positioned the membership categories as the claims-makers rather than specific individuals. Although this erased some of the nuance and specificity of the individual claims, it was necessary in order to identify common trends and patterns in the data; categorizing grounds, warrants, and conclusions based on their themes confirmed that those themes were prominent throughout the data and that they were not only used by a small number of individual claims-makers. Additionally, one of my objectives was to determine if or how claims had changed over time, so when I realized that very few newspaper articles were written during or after Bill C-30, the focus of my research shifted to parliamentary records, which included discussions and debates about Bill C-46 and Bill C-47. However, Bill C-46, Bill C-47, Bill C-50, Bill C-51, and Bill C-52 were put forward during the 40th Parliament of Canada, while Bill C-30 and Bill C-13 were proposed in the 41st Parliament of Canada; an election had taken place and several

Members of Parliament (MPs) who had spoken about the earlier bills were not present to discuss the later bills. Their statements could not be used to determine if claims had changed over time. Studying the claims of membership categories preserved the continuity of the claims even if the individual members changed. Finally, identifying common grounds, warrants, conclusions, motifs, and other rhetorical strategies across different claims-maker groups in order to gain a better understanding of the broader discourse – and how it might relate to the discourse of surveillance and privacy in general – was more important than tracking individual opinions.

There were some difficulties with more diverse condition categories. While the claims of specific political parties were consistent as matters of party policy, legal experts, members of civil society, and journalists had more diverse opinions and did not present a united rhetorical “front.” The conflicting claims produced within these groups were still useful to the analysis because they illustrated the way these groups socially constructed the meaning of lawful access through rhetorical “competition,” and the various claims could still form around motifs that were prevalent within the group, forming sub-groups. The focus of the analysis remained on membership categories rather than specific individuals.

Next, the statements were organized according to the rhetorical idioms they expressed. During the initial readings of the data, all rhetorical idioms were considered. However, only two were retained for the final analysis: the rhetorical idiom of endangerment and the rhetorical idiom of loss. These two rhetorical idioms were chosen as the focus of the analysis based on a subjective qualitative assessment of the data. They were found to encompass a significant amount of data highly relevant to the construction of social problems relevant to lawful access legislation and they were both consistent with the broader research on security and surveillance.

The rhetorical idiom of endangerment included statements that discussed threats to Canadian society, such as new technologies, (cyber)crime, or cyberbullying, or that discussed solutions to those threats, such as lawful access legislation. The way claims-makers used this rhetorical idiom was consistent with research that shows how states use threats and risks to justify and expand security measures (see Akdeniz, 2002; Etter, 2001; Lyon, 2003; Mathiesen, 2013; Pallaras, 2011; Baker, 2003; Bannister, 2005), and although these studies cannot be used to validate or reject claims according to social problem theory, they can be used to situate the claims made about lawful access legislation within the broader context of studies on security, surveillance, and privacy. Thus, the explicit statements made about the existence of putative threats and the academic research on the subject both provide evidence that the rhetorical idiom of endangerment can be used to analyse the rhetoric claims made about lawful access legislation.

The rhetorical idiom of loss included statements that discussed the erosion or devaluation of privacy rights, including statements that privacy rights would be devalued, that privacy rights should be protected, or that privacy rights would be protected. Regardless of their position, they were all statements that pertained to the topic of privacy rights. As with the rhetorical idiom of endangerment, the inclusion of the rhetorical idiom of loss is also supported by the broader literature; privacy rights are important to democracy and political activity (see Godfrey and Simbarashe, 2025; Hong and Kim, 2021; Mladenov and Galetin, 2025; Pandey, Gupta, and Chattopadhyay, 2020; Schaaf and Quiring, 2023; Scheffauer, Goyanes, and Gil de Zúñiga, 2021; Velasquez and LaRose, 2015), and they are often eroded in favour of security (see Baker, 2003; Bannister, 2005; Lyon, 2003; Mathiesen, 2013). The decision to use the rhetorical idiom of loss during coding is therefore justified by both the claims contained in my data and in the literature on privacy rights.

The final part of the coding focused on the rhetorical motifs used to construct the idioms of endangerment and loss. While claims-makers used the rhetorical idioms to create the condition-categories that defined the endangerment of society and the loss of privacy, the motifs represent the vocabulary used by claims-makers to describe the social problems related to lawful access legislation in more detail.

The majority of the motifs during coding were explicitly stated by claims-makers and were therefore easy to identify. The definitions provided below were used when the motifs were not explicitly stated, such as when they were implied based on the context. Each motif was associated with the idiom of endangerment or the idiom of loss. Statements were coded according to these categories to determine which rhetorical motif they expressed.

The motif of new technologies included all statements made about modern technologies, particularly telecommunication technologies such as the internet.

The motif of old crimes included all statements made about crimes that existed before and independently of new technologies, but that were often facilitated by new technologies.

The motif of new crimes included all statements made about crimes that depended on the existence of new technologies and could not be committed about them.

The motif of cyberbullying included all statements made about harassment or threats against certain individuals, either by contacting them directly, by spreading information about them, or by spreading images of them, so long as the harassment was conducted with the use of modern technologies.

The motif of protection included all statements that something needed to be protected or would be protected.

The motif of obligation included all statements that presented a course of action is a matter of necessity.

The motif of vulnerable children included all statements made about specific threats made against children or statements that children were specifically vulnerable to a threat.

The motif of democratic civil rights included all statements that defined privacy as an inherently important right necessary to democratic society.

The motif of oversight included all statements about the requirements for lawful access requests, restrictions on lawful access requests, the reporting of lawful access requests, the transparency of lawful access requests, or the general supervision of lawful access.

The motif of political partisanship included all statements made about an individual's affiliation with an official political party in the House of Commons.

The motif of the balance between security and privacy included all statements made about the need to maintain a proportional balance between security necessary used to protect the public and privacy rights that are necessary to democratic society.

The motif of trivialization included all statements that personal information was unimportant, non-private, or too limited to provide meaningful personal details.

The motif of normalization of new surveillance measures included all statements that compared lawful access to older surveillance methods that existed before modern technologies in order to make them seem similar. This category included statements that established similarities between the oversight of lawful access and the oversight of older surveillance methods.

These rhetorical motifs contained more detailed information about how claims-makers socially constructed the social problems surrounding lawful access legislation. Because the motifs represent the vocabulary used in the rhetoric, they revealed important trends in the data, and they also made it easier to identify common grounds shared between proponents of lawful access legislation and privacy advocates. Additionally, the motifs clearly identified elements of vocabulary that were shared by claims-makers, but that were defined differently, as these motifs were used to make contradicting claims. This allowed me to better analyze how different claims-makers rhetorically constructed the putative social conditions of endangerment and loss.

Conclusion

Social problem theory's constructionist perspective offers an excellent framework to study the development of lawful access legislation in Canada. By defining social problems based on claimants' claims-making activities, the theory arguably offers more "objective" criteria than positivist theories can manage; the construction of claims is the construction of social problems, and the researcher is not forced to establish arbitrary and subjective standards to determine whether or not social conditions are a social problem that truly exists in an objective sense. Moreover, the four stage natural history model is a very useful tool to study how the rhetoric of a social problem evolves over a longer period of time and how different claimants respond to each other according to their own perspectives and their own relationship with the social problem. The theory emphasizes that social problems are "not static conditions, but sequences of events" (Spector and Kitsuse, 1973, p. 146) that "develop over time and may be characterized by different activities at different times in their development" (Spector and Kitsuse, 1973, p. 147-48). To supplement the four stage natural history model, the construction of claims through their grounds, warrants, conclusions, motifs, rhetorical idioms, and moral condition-categories

provides a smaller-scale instrument of study to analyze the content and meaning of specific claims. Together, the two concepts can be used to better understand how claims-making rhetorics – and the putative social conditions constructed by their claims – persist or change over time.

Although there are some epistemological debates and disagreements about how strictly social problem theory should adhere to its constructionist perspective, my research follows a hard reading of the theory and focuses solely on the claims-making process. However, I borrow from Bogard (2003) to examine the context of the social problems that surround lawful access, not to question the validity of the claims, but to extend the claims into a broader criminological, legal, and political context in order to better understand the recurring rhetorical motifs and rhetorical trends used in the claims' construction.

With this in mind, my research studies the claims made about lawful access legislation in order to answer the following questions:

First, how did claims-makers use rhetorical idioms and motifs to make claims about lawful access legislation?

Second, how did the claims produced by claims-makers construct social problems?

Third, how can the claims produced by claims-makers about lawful access provide a greater understanding of the broader body of research on security, surveillance, and privacy?

Chapter 3: Endangerment from New Technologies

Security risks such as crimes and terrorism are a prominent part of the discourse of surveillance, with policymakers routinely citing terrorism (Lyon, 2003; Mathiesen, 2013) and cybercrime (Akdeniz, 2002; Etter, 2001; Pallasas, 2011) as reasons to implement new surveillance measures in order to maintain the “balance” between security and civil rights (see Baker, 2003; Bannister, 2005; Neocleous, 2007). This concern for safety and risk is particularly interesting from a criminological perspective because of how it can be related to broader fears of crime. Importantly, Smith and Hill (1991) argue that “fear of crime is not always (if even typically) the product of objective probabilities with respect to risk, but instead reflect perceived vulnerabilities that often correlate poorly with actual risk” (p. 315), which situates fear of crime within my methodology as a social problem based on the putative risk of crime constructed through claims-making activities and allows me to interpret my data in the context of terrorism and cybercrime not only as risks, but as risks that elicit public fear.

Within the context of social problem theory’s rhetorical focus, the discourse of (cyber)crime, terrorism, risk, and fear is best understood through the rhetorical idiom of endangerment, a rhetorical strategy used to construct threats to health or safety (Ibarra and Kitsuse, 1993) in order to claim the existence of a social problem. As the data examined in this chapter shows, claims-makers who supported lawful access cited threats to Canadians’ health and safety as grounds to claim that crimes, particularly crimes associated with new technologies, were a social problem that would be solved by implementing new lawful access legislation. Thus, the subject of this chapter is the rhetorical idiom of the endangerment of Canadian society from new technologies.

To better analyze the rhetorical idiom of endangerment within the context of fear of cybercrime associated with new technologies, this project borrows from Jackson and Gray's (2010) study of functional and dysfunctional reactions to the fear of crime,¹⁷ and how the reaction to the fear of crime can positively or negatively affect quality of life depending on how it is managed on an individual level. I also consider Hollway and Jefferson's (1997) argument that the fear of crime and the risk of victimization "must be addressed in the political context of how multifarious risks are known and regulated" (p. 258) and that "discourses that appear to promise a resolution to ambivalence by producing identifiable victims and blameable villains are likely to figure prominently in the State's ceaseless attempts to impose social order" (p. 265). Keeping the works of Smith and Hill (1991), Jackson and Gray (2010), and Hollway and Jefferson (1997) in mind, the question then becomes how the rhetorical idiom of endangerment, as an act of (political) claims-making, created fears about crime associated with new technologies in order to support certain claims about and reactions to those crimes. Although Jackson and Gray (2010) studied individual reactions to crime, I argue that the concept of a functional or dysfunctional reaction to crime can be used to interpret the claims made about new technologies as a form of endangerment.

The data presented throughout this chapter demonstrates how the claims-making activities of lawful access legislation's proponents leveraged the fear of crime to create support for their conclusion. First, I examine how the claims-makers established grounds that new technologies were a cause of crime to leverage the fear of crime and define new technologies as

¹⁷ Jackson and Gray (2010) define functional reactions to crime as worries about crime that encourage individuals to take precautions about their personal safety and do not affect their overall quality of life, and define dysfunctional reactions to crime as worries about crime that do have a negative effect on an individual's quality of life, either because of the worries themselves or because of the precautions the individual uses to protect themselves from crime.

a putative social problem through the rhetorical idiom of endangerment. Following this, I demonstrate how the motif of protection, combined with the motifs of obligation and vulnerable children, were used to build the rhetoric by using the dangers of new technologies to justify government intervention. Finally, I examine how the grounds that new technologies are a cause of crime and the warrant that the government had to protect Canadians were used to support the conclusion that lawful access legislation was the necessary solution to the problem.

Grounds

This section examines the rhetorical grounds used to support the claims that new technologies were a danger to Canadian society, starting with the way new technologies (putatively) changed crimes by providing more effective means to commit “old” crimes or by creating “new” crimes aimed at the technology itself, as explained in a document written by the Canadian Association of Chiefs of Police (CACP):

These same technologies are providing a safe haven for serious criminal activity in Canada – organized crime, sexual predators, gangs, identity theft and terrorism are among the many examples. New technologies allow for old crimes to be committed in new ways, as well as new crimes to develop, including viruses, trojans, worms, hacking, spyware, spam, phishing, identity theft, Internet fraud and money laundering. (Canadian Association of Chiefs of Police, n.d., p. 1)

Building on this, the chapter next discusses cyberbullying, which is treated as a distinct issue because of its overlap with both new and old crimes and because of its significant prominence in the rhetoric. Finally, it discusses how claims-makers who held different stances on lawful access legislation treated the rhetorical idiom of endangerment from new technologies as common

grounds, and how these common grounds affected the rhetorical construction of lawful access legislation.

Old Crimes and New Technologies

In the rhetorical idiom of endangerment from new technologies, claims-makers argued that new technologies would facilitate “old” existing crimes and increase the risks faced by Canadians. As police representative Joe Oliver put it, “[w]hen it comes to cybercrime, it is important to note that cybercrime is, in many cases, a modern means to commit familiar crimes [...] such as fraud, identity theft, and other financially motivated crimes” (Oliver, 2014, p.5) and research shows that new technologies are involved in a wide range of crimes, such as film piracy (Wang and Zhu, 2003), industrial espionage (Fitzpatrick and DiLullo, 2013; Helms, Etkin, and Morris, 2000), intimate partner aggression (Booth, Derefaka, Khan, and Brewer, 2023), stalking (Fox, Coupland, and Hart, 2024), and child sexual abuse material (Eggstein and Knapp, 2014; Lirëza, and Koçi, 2023; Marit, Şargu, and Corsei, 2022). Although these studies are not directly relevant to the claims-making activities discussed in this chapter, they are evidence that the grounds cited by claims-makers to construct the rhetorical idiom of endangerment from new technologies can provide insight into the broader discourse of security, surveillance, and (fear of) crime; the rhetoric discussed here is not exclusive to lawful access legislation and can be applied to other forms of surveillance.

To support the rhetorical idiom of endangerment, claims-making activities that focused on the way new technologies facilitate old crimes generally sought to establish a direct link between the use of technology and its human victims, as is the case in the following quote by police representative Joe Oliver:

When it comes to cybercrime, it is important to note that cybercrime is, in many cases, a modern means to commit familiar crimes. For example, criminals create and deploy malicious software programs to steal passwords or to obtain personal and financial credentials. This information then allows them to commit a number of offences, such as fraud, identity theft, and other financially motivated crimes. (Oliver, 2014, p.5)

This excerpt begins by explaining how malicious software can affect computers, which would be tied to new crimes that target modern technologies. However, it then explains how the malicious software can be used to commit older crimes such as fraud, identity theft, and other financial crimes that directly affect human victims. The technology is primarily presented as an intermediary that allows criminals to victimize individuals rather than a victim of new crimes. In this particular rhetoric, “new” crimes that negatively affect new technologies are deemed insufficient to the rhetorical idiom of endangerment. A human victim is required to establish the grounds that new technologies pose a danger to society.

According to (Spector and Kitsuse, 1973), an effective claims-making process should communicate a concrete and specific sense of dissatisfaction which should be attributed to a clear target to clearly establish that the social problem exists and that the claims-makers can provide a solution. Likewise, Hollway and Jefferson (1997) argue that establishing clear victims and victimizers is an important part of the political discourse that surrounds the fear of crime. In the grounds discussed above, the dissatisfaction is the danger posed by new technologies, but “new ways to commit old crime” and “new crimes” are both broad, abstract terms that lack specificity and thus fail to define a salient point of dissatisfaction. Linking crimes to human victims addresses this to a certain extent, but still lacks a clearly-defined sense of attribution.

Moreover, some claims-makers shifted the use of technology into the past – before it was available – to further emphasize the dangers it posed. One of the witnesses asked to testify about Bill C-13 was Gregory Gilhooly, a lawyer who was himself a victim of grooming. Recounting his experiences, he stated the following:

Graham [James] took advantage of me back in the days before the Internet. I was groomed over any number of months, almost a year by Graham. Had what happened with Graham taken place in this environment, I'm sure the Internet would have been involved and there would have been a grooming process that involved an online component. Back then it was very much face to face. We didn't even have voicemail machines back then. (Gilhooly, 2014b, para. 291)

By Greg Gilhooly's own admission, the crimes he suffered took place before internet use was widespread, yet his comments assert – and establish the grounds – that technology would have undoubtedly been involved if it had been available at the time, attributing the danger of child predators to new technologies while providing another concrete and specific instance of dissatisfaction. This testimony was later referenced by Conservative MP Robert Goguen, who described Gilhooly as “un avocat qui a été victime d'un cyberprédateur pendant sa jeunesse” (Goguen, 2014, p. 8510) – a lawyer who had been victim of a cyberpredator in his youth. The rhetorical grounds changed from “the internet was not involved” to “the internet would have been involved if it had been accessible” to “the internet was involved” in order to provide grounds that can better support the claim that modern technologies are criminogenic; in a manner consistent with social problem theory, the putative social conditions associated with new technologies are what matters to the claims-making process, and claims-makers can construct the role of new technologies according to what best supports their claims.

As a rhetorical motif, old crimes facilitated by new technologies were used to insert technology into the danger-based relationship between criminals and their victims. In doing this, the grounds framed the technology not simply as a neutral mediator, but as an aggravating factor. According to police representative Joe Oliver, technology “allows” (Oliver, 2014, p.5) criminals to commit offences. Similarly, Gregory Gilhooly described Graham James’ crimes as “very much face to face” (Gilhooly, 2014, para. 291), yet stated that Graham James would have used modern technologies to groom his victims if such technologies had been widely available at the time – implicit grounds that Graham James’ crimes were limited by the need to maintain direct contact with his victims and that modern technologies would have made him more dangerous by allowing him to commit his crimes without such limitations.

The grounds that new technologies posed a danger to Canadian society because of the way they enabled and aggravated old crimes demonstrate how social problems are constructed based on putative social conditions rather than “objective” facts. According to claims-makers, the possibility that new technologies could be used to commit old crimes is sufficient grounds to claim they are a social problem, much like Smith and Hill (1991)’s argument that fear of crime is based on perceived risk than actual risk.

New Crimes for New Technologies

While the rhetorical motif of old crimes focused on how new technologies would increase existing criminal risks, the motif of new crimes established the grounds that new technologies would create new risks to Canadian society. This was expressed in one instance by Conservative MP Randy Hoback, who said that that “[t]echnology has [...] introduced us to new crimes that simply did not exist before there were computers” (Hoback, 2014, p. 4573) and a document submitted to Public Safety Canada by the CACP provided a more detailed list of new

crimes that included “viruses, trojans, worms, hacking, spyware, spam, phishing, identity theft, Internet fraud and money laundering” (Canadian Association of Chiefs of Police, n.d., p. 1).

Though identity theft, fraud, and money laundering could be considered old crimes aggravated by the new technologies, their inclusion here is informative because it shows that, in some cases, claims-makers believed that technological involvement could modify an existing crime in such a way that it became something new. The way the grounds connect new crimes to old crimes – much like how motif of old crimes connected the criminal use of technology to human victims – is also interesting because it illustrates how claims-makers sought to create a sense of threat.

Though viruses, hacking, and spyware are a danger to new technologies on their own, they are not necessarily a danger that the general public should be concerned about compared to crimes such as identity theft or fraud.

The need to ground the threat in terms of human victims would also explain why new technologies were not a prominent part of the claims-makers’ grounds. Though claims-makers occasionally referenced these new crimes that could only exist because of new technologies, there is little data on the subject to analyze. Nevertheless, the rhetorical motif of new crimes created by new technologies is important because of the way it contrasts with the motif of mold crimes aggravated by new technologies and because it provides additional context to the motif of cyberbullying, which was an extremely important motif within the grounds of the idiom of endangerment from new technologies.

Cyberbullying

Claims-makers mobilized the motif of cyberbullying as grounds to establish the dangers of new technologies, making it a critical element of their rhetoric that combined aspects of old

and new crimes associated with modern technologies. As NDP MP Pierre Nantel described cyberbullying while discussing Bill C-13:

Ce sujet, c'est celui de la cyberintimidation. C'est l'intimidation traditionnelle de la cour d'école, à visage découvert, qui se poursuit maintenant après les classes de façon beaucoup plus sournoise, souvent de façon complètement anonyme. C'est une forme d'intimidation qui, par sa nature même, dure non pas de 9 heures à 17 heures, mais 24 heures sur 24. C'est une espèce de violence qui n'offre aucun refuge parce que ses victimes savent qu'elle continue même quand on s'en cache, même quand on essaie d'y échapper. (Nantel, 2013, p. 1569)

The putative grounds established by Pierre Nantel are based on the motif of old crimes, citing the bullying that takes place in schools and how it could be extended outside school hours, making it impossible for victims to escape. Comparatively, Liberal MP Wayne Easter emphasized the technological aspect:

The principal incentive behind this legislation has been the growing problem of cyberbullying, which has led to some tragic consequences. There is no question cyberbullying is a scourge on our society and that cyberbullying is a particular strain on our young people. We could go through all kinds of cases of that, and other speakers have. The Liberals are supportive in principle of legislative measures that would provide law enforcement with additional tools to combat cyberbullying. This is an area where the Criminal Code urgently needs to be updated to reflect the realities of modern technologies. (Easter, 2014a, p. 8117)

Though the grounds established by Wayne Easter did not describe cyberbullying in specific terms that would position it as an old or new crime, they did clearly emphasize the putative need

to update the Criminal Code in a manner that is consistent with the motif of new crimes. It is therefore reasonable to say that the grounds found in the data associated cyberbullying with both old and new crimes associated with modern technologies. Police representative Joe Oliver commented on this:

As identified by the cybercrime working group of the coordinating committee of senior officials, bullying and cyberbullying may be manifested in a range of criminal offences, such as criminal harassment, uttering threats, or intimidation. High-profile cyberbullying incidents have taught us that bullying may be facilitated and amplified by telecommunication. As it stands, the existing provisions in the Criminal Code regarding offences of false, indecent, or harassing communications do not currently reflect the increasingly ubiquitous role of telecommunication as a possible medium to bully individuals in a criminal capacity. (Oliver, 2014, p. 6)

These grounds acknowledged that cyberbullying could be included under existing crimes such as harassment, uttering, or intimidation, but also stated that these laws did not accurately reflect how technology was used to perpetuate cyberbullying. Accordingly, cyberbullying occupied a specific place in the rhetoric, existing at the intersection of the motifs of old and new crimes while constituting its own rhetorical motif within the idiom of endangerment.

Claims-makers who were part of the Conservative government also included the motif of cyberbullying as a prominent component of their rhetoric. While discussing how the measures contained in Bill C-13 would address the problem of cyberbullying, former Justice Minister Peter MacKay said the following:

Turning first to the issue of cyberbullying, as I mentioned, the bill proposes a new Criminal Code offence prohibiting the nonconsensual distribution of intimate images.

Essentially this offence would prohibit the sharing of sexual or nude images, as defined, without the consent of the person depicted. It is a very nasty, cruel attempt to humiliate or worse, and has, as I mentioned, a pernicious effect that has become all too prevalent, particularly amongst young people. (MacKay, 2014b, p. 1)

Currently, the Criminal Code can in fact address most of the serious forms of cyberbullying through, for example, existing offences of criminal harassment per section 264, uttering threats per section 264.1 or identity fraud, found in section 403. However, there is no offence in the Criminal Code that specifically addresses the contemptible form of cyberbullying that has emerged, involving the distribution of sexual images without the consent of the person depicted in that image. (MacKay, 2013, p. 1436)

These statements, like Joe Oliver's, explicitly acknowledged that the Criminal Code did have laws against some aspects of cyberbullying, such as harassment, uttering threats, or identity theft, that could be used to police some forms of cyberbullying. However, they noted that there was one specific element of cyberbullying – “the nonconsensual distribution of intimate images” – that was not part of the Criminal Code and had to be added to the law, reinforcing the grounds that the Criminal Code was not able to criminalize the full range of behaviours associated with cyberbullying.

Additionally, Peter MacKay's statements show how proponent of security and surveillance utilize threats to support their claims. The grounds that the Criminal Code did not sufficiently criminalize cyberbullying behaviours created a threat using the rhetorical idiom of endangerment from new technologies and synergized with the grounds that lawful access legislation *would* criminalize these behaviours. The presence of a threat is sufficient to construct a social problem, but as the claims-makers' objective was to implement lawful access legislation,

the threat of cyberbullying had to be specifically associated with that legislation in order to provide rhetorical support for the claim that lawful access would solve the social problems of cybercrime, cyberbullying, and other threats related to new technologies.

The motif of cyberbullying is also important because it allowed claims-makers to add more specificity to their rhetoric and create a more defined sense of threat. At the time of Bill C-13, cyberbullying became an extremely prominent motif in the data as it was associated with the deaths of Rehtaeh Parsons, Amanda Todd, and Todd Loik, three victims of cyberbullying who committed suicide after the abuse they suffered:

We have heard of cases involving Rehtaeh Parsons in my province of Nova Scotia, Amanda Todd on the west coast, a young man named Todd Loik in Saskatchewan recently, and countless others. It is clearly a case of the worst form of harassment, intimidation and humiliation of young people, which resulted in a feeling of hopelessness, that there was no other way out, and they took their lives. (MacKay, 2013, p. 1436)

The parents of two victims – Carol Todd, mother of Amanda Todd, and Glenford Canning, step-father of Rehtaeh Parsons – testified before the House of Commons' Standing Committee on Justice and Human Rights:¹⁸

I often talk about Amanda's story as the perfect storm. Her life from ages 12 to 15 encompassed the following areas: sextortion, bullying online and offline, cyber-harassment, mental health that included depression and social anxieties, learning challenges, and a medical diagnosis of ADHD. There were also ongoing moves from school to school that resulted in unstable peer relationships. The once bubbly daughter I

¹⁸ Glenford Canning also spoke before the Standing Senate Committee on Legal and Constitutional Affairs.

had become reclusive and quiet. Unfortunately, Amanda was no longer able to handle the stress of what was going on around her. (Todd, 2014, p. 1)

My name is Glen Canning. In April 2013, my daughter Rehtaeh Parsons ended her life following a very traumatic sexual assault and months of cyber-harassment. The worst part of the harassment she endured involved a photo that was spread by text messaging and on social media. (Canning, 2014, p. 4)

This marked a significant change in the way the grounds were presented. While cyberbullying was mentioned prior to Bill C-13, the rhetoric that framed previous bills discussed cyberbullying and related cybercrimes in relatively vague terms, as seen in these quotes discussing Bill C-46:

The unfortunate part is that what I have had to investigate today is cyberbullying. Cyberbullying is basically text messaging or other forms of verbal abuse toward another student or individual. It could be by a group of people bullying one child. Many times that one child has no avenue. I have seen action being taken by the schools, and they are helpless without having this bill passed, to battle cyberbullying. This legislation is needed and we need to get it through to help protect the future generations of Canadians. (Clarke, 2009, p. 6191)

Internet child pornography¹⁹, for example, has become a \$2.6 billion industry. The latest RCMP estimates indicate that there are 60,000 identified IP addresses in Canada accessing child pornography. People may be surprised to know this but the National

¹⁹ Randy Kamp's comments are relevant because the perpetrators in the Parsons case were convicted of distributing child pornography (Segal, 2015), and provide another example of how claims-makers positioned cyberbullying at the intersection of old and new crimes associated with modern technologies. Though claims-makers established the grounds that cyberbullying behaviours were not all criminalized, they also identified some that were.

Centre for Missing and Exploited Children documented that 85 children are reported missing every hour, not every day, every week or every month, but every hour, totalling more than 750,000 missing in a year. Many cases involve luring schemes facilitated online. (Kamp, 2009, p. 6204)

Conservative Rob Clarke's comments above-described cyberbullying almost as a hypothetical scenario: it could include text messages or verbal abuse, the victim could be a student or another individual or a child, it could be done by a group of people, actions taken by schools are unspecified. There is an implication that specific cases of cyberbullying did take place, but not enough firm details to refer to any specific crime. Likewise, Randy Kamp linked internet child pornography to abduction, but did not point to any one specific criminal incident.

In comparison, the participation of Carol Todd and Glenford Canning in the rhetoric of Bill C-13 led to a more defined construction of the social problem: specific victims were named, the circumstances were described in detail, and there was someone to blame for the crime. This is important because claims that are general and more diffuse are less likely to be recognized and are less likely to lead to the claims-makers' proposed solution (Spector and Kitsuse, 1973). By mobilizing the (widespread) occurrence of cyberbullying and statistics about the broad scope of child pornography as grounds, Clarke and Kamp sought to establish the claim that new technologies were a danger to society, but Carol Todd and Glenford Canning provided more convincing grounds for the claim due to their specificity. The use of cyberbullying within the grounds during Bill C-13 combined the dangers of old and new crimes with specific criminal cases and victims that clearly defined the problem and assigned responsibility to individual criminals rather than an abstract threat. This created a much more tangible sense of

dissatisfaction than earlier claims and better conveyed the putative danger posed by new technologies.

The empirical scope of the grounds is not the most important point of credibility, and it may not be relevant to the grounds' credibility at all. As seen in the rhetorical evolution of Graham James – who was a child predator, then a *potential* cyberpredator limited only by the fact that the technology that could have facilitated his crimes was not available when those crimes took place, then an *actual* cyberpredator according to Conservative MP Robert Goguen – convincing facts are more important to the claims-making process than empirical facts. The rhetorical idiom of endangerment from modern technologies presupposes that technology is present in criminal activity somehow and seeks to establish that the danger is a personal one in order to elicit a more convincing fear of crime. By mentioning specific crimes and victims, claims-makers were able to construct a more salient social problem and lend additional credibility to their claims, even when they were relying on imaginary grounds which were made real through the claims-making process.

Common Grounds

Supporters of lawful access legislation used the rhetorical idiom of endangerment and the motifs of crime and cyberbullying to construct new technologies as a social problem that could be resolved by implementing new lawful access legislation. This rhetoric is consistent with the way cybercrime is used to justify new surveillance measures (see Akdeniz, 2002; Etter, 2001; Pallaras, 2011) in order to balance security needs and civil rights such as privacy (see Baker, 2003; Bannister, 2005). This often results in a loss of privacy rights (Bannister, 2005; Pozen, 2016), and the grounds used to construct the rhetorical idiom of endangerment for new technologies can explain, at least in part, why this is the case.

All groups of claims-makers agreed that crimes associated with new technologies posed a threat to Canadian society. In 2009, Liberal MP Scott Simms said that “certainly with the advent of technology and social networking on the Internet, [cyberbullying] is a very pertinent issue” (Simms, 2009, p. 6190), and Bloc Québécois MP Guy André expressed concerns about cybercrime: “Avec l'expansion de l'Internet et de la technologie numérique, la cybercriminalité est devenue une menace de plus en plus importante” (André, 2009, p. 6214). Drawing on his own experiences with the legal system, NDP MP Jonathan Genest said in 2013 that “[l]orsque j'ai commencé à plaider à l'aide juridique en 2005 ou en 2006, si je ne me trompe pas, il y avait déjà de la cybercriminalité” (Genest-Jourdain, 2013, p. 1561).²⁰ The data shows that, from 2009 to the debates about Bill C-13 that took place in 2013 and 2014, members of the Bloc Québécois, Liberal Party, and New Democratic Party – the parties that acted as the elected opposition to the Conservative Party while they, as the governing party, were working on lawful access legislation – agreed that crimes associated with new technologies posed a danger to society.

The general agreement among claims-makers that new technologies were a threat is important because it constitutes a common ground – grounds that are accepted by the different parties involved (Toulmin, Rieke and Janik, 1984) – between claims-makers. While the effects of lawful access legislation on privacy rights were contested to some extent,²¹ the grounds that new technologies exacerbated crimes and cyberbullying were not. Since the threat of new technologies was accepted as a social problem by all political parties, it would have been extremely difficult for them to claim that there was no social problem and that lawful access

²⁰ These concerns existed even before 2009. In 2005, Liberal MP and Public Safety Minister Anne McLellan was quoted saying that criminal organizations used new technologies to “to conceal what they do, to move their laundered money, to traffic in humans, to traffic in drugs, to traffic in guns, and we have to be able to intercept their communications to break up those kinds of networks.” (Campbell, 2005, para. 12).

²¹ Claims that lawful access legislation would cause a loss of privacy rights are discussed in chapter 4. Claims that lawful access legislation would instead protect privacy rights are discussed in chapter 5.

legislation was necessary.²² Expanding this to the broader discourse on the subject, it would explain why the balance between security and civil rights so often favours security measures at the expense of democratic rights; if policymakers and privacy advocates accept the (putative) fact that there are security risks, they cannot logically claim that security measures are unnecessary.

Domain and Orientation

The grounds used to establish a claim define social problems through domain statements that “examine phenomena and determine which do, and which do not, fall within the defined category's domain” (Best, 1987, p. 104) and orientation statements that “guide the way we interpret the problem, suggesting appropriate avenues for response” (Best, 1987, p. 105). Thus, by associating old crimes, new crimes, and cyberbullying with new technologies, claims-makers situated the social problem of endangerment discussed in this chapter within the domain of new technologies. According to the grounds mobilized by proponents of lawful access legislation – and some claims-makers who expressed some measure of resistance to the legislation – new technologies facilitated and exacerbated old crimes, new technologies created entirely new crimes that could not exist without it, and new technologies made cyberbullying a pervasive threat.

Though the domain emphasized the criminogenic role of technology, proponents of lawful access were oriented towards a legal solution: lawful access legislation. The legislation would, according to the claims-makers who supported it, provide the legal changes necessary to

²² The way the rhetorical strategies favoured lawful access legislation over privacy rights is discussed further in the conclusion, as it requires the full context of the research.

allow the government to better investigate modern telecommunication technologies when they were used to commit criminal activities. As stated by Conservative MP Robert Goguen:

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, the Mutual Legal Assistance in Criminal Matters Act, and Canada's anti-spam legislation. This bill would also incorporate in the Competition Act, by reference, the new powers in the Criminal Code regarding preservation demands, preservation orders, and production orders for historical transmission data so that they could be used in investigations of all conduct under the Competition Act, both criminal and civil. As is the case throughout the bill, preservation and production orders sought by the bureau would be subject to judicial oversight. (Goguen, 2014, p. 8511)

According to these grounds, lawful access legislation would update relevant laws to make them “technology neutral” and thus applicable to new technologies, while also allowing investigators to request that information be preserved and produced as needed. This would allow to state to monitor the use of new technologies through legal means rather than controlling the infrastructure on a more technical level.

Additionally, the legal orientation of their rhetorical grounds allowed proponents of lawful access to expand the legislation’s role beyond granting the state greater access to personal information:

The non-consensual distribution of intimate images can literally take lives. I cannot emphasize enough, as my friend has said and Mr. Canning and others have said, the urgency with regard to moving the legislation forward, putting in place those necessary protections found in the Criminal Code and giving the police the power to intervene and

pre-empt and prevent the type of activity that led to the death of Rehtaeh Parsons, Amanda Todd and others. (MacKay, 2014b, p. 8108)

Such grounds served to blur the distinction between lawful access legislation as a means to obtain personal information and lawful access legislation as a means to criminalize (technology-related) acts considered harmful to society, such as cyberbullying. By rhetorically conjoining the two issues, proponents of lawful access were able to claim that the legislation was necessary in order to prevent crime. A strictly technological orientation of the grounds would not have been able to support this rhetoric as effectively because it would have been limited to surveillance and investigate powers. While these could have still been used to claim that the legislation would protect Canadians by supporting police investigation, criminalization provided a more direct link between lawful access and crime prevention and made it more difficult for claims-makers who were concerned about privacy rights to oppose the legislation.

As evidence of the rhetorical effects of combining lawful access and the criminalization of cybercrimes and cyberbullying, members of the opposition parties attempted to split Bill C-13 so the surveillance measures and the criminalization measures could move through the legislative process separately:

However, at the beginning I said I am pleased, but I am also troubled. I am troubled because tagged onto the bill were measures of the old Bill C-30 on lawful access that so many Canadians spoke out against. Efforts were made to split the bill at committee and yet, despite the urging of the new Privacy Commissioner and many other witnesses, including Carol Todd, the bill was not split. (Easter, 2014b, p. 8516)

As I mentioned before, only a few pages of this 70-page omnibus style bill are directly related to cyberbullying. Yesterday the NDP proposed what I think is a very smart

legislative solution. Our justice critic proposed splitting this bill in two. The cyberbullying provisions would be removed from Bill C-13 and put into a separate bill that could be expedited through the legislative process. In this way, the justice committee could take the appropriate amount of time to study other provisions contained in Bill C-13. I am disappointed that the Conservatives rejected this very logical proposal.

(Donnelly, 2013, p. 1524)

Dividing the legislation in this manner would have allowed the opposition to support the criminalization of cyberbullying without also supporting surveillance measures that could undermine privacy rights, which shows that all claims-makers agreed on a legal solution to the problems caused by new technologies. The disagreement is rather on how the domain was defined, with some proponents of the legislation including surveillance and information requests while privacy advocates sought to exclude surveillance in order to focus specifically on cyberbullying and cybercrime.

Preserving the relationship between lawful access and criminalization, the Conservative government rejected calls to split the legislation on the grounds that separating the technological aspects from the strictly legal provisions pertaining to the Criminal Code would not provide a solution to the problem:

That is what we are attempting to do through this bill. It is modernizing it. It is moving us into the 21st century, into the modern age of technology. That is what we are doing. To suggest that we should split the bill and put the Criminal Code sections in one part and put the police powers in another is like saying we should give somebody a paddle but not a boat. (MacKay, 2014a, p. 8110)

Proponents of lawful access legislation established the grounds that the surveillance measures contained in lawful access and the criminalization of cyberbullying and other crimes were both integral and necessary components of the legislation, and that they were both required in order to remedy the social problems putatively caused by new technologies.

These domain and orientation statements provide a concrete example of how security threats and fear of crime are used to support surveillance in a more general context. Proponents of lawful access did not simply claim that the legislation was necessary because new technologies endangered Canadian society. The rhetorical grounds they expressed situated the danger in the domain of new technologies and oriented it towards a legal solution offered by surveillance combined with criminalization. This made it difficult, if not impossible, for the opposition parties and privacy advocates who agreed that new technologies were a danger to society to reject lawful access legislation entirely. Common grounds shared between proponents and opponents of lawful access legislation agreed that the putative dangers posed by new technologies were a social problem. Because of this, opponents of lawful access were rhetorically bound to demand a solution to the problem they had recognized. However, because they also claimed that lawful access legislation would cause a loss of privacy rights,²³ they could not support the legislation. Thus, they were positioned between two opposing rhetorical positions. The opposition parties attempted to resolve this conflict by requesting that the legislation be split, but since the Conservative government refused to do this, opponents were essentially forced to make a choice and prioritize either the rhetorical idiom of endangerment from new technologies or the rhetorical idiom of loss of privacy. This supports Pozen's (2016) argument that "[p]rivacy is constantly being juxtaposed with competing goods and interests,

²³ These claims are analyzed in chapter 4.

balanced against disparate needs and demands” (p. 222) and explains why privacy rights are so often sacrificed for the sake of security (see Baker, 2003; Bannister, 2005; Lyon, 2003; Mathiesen, 2013). The rhetorical construction of lawful access legislation shows that when privacy advocates agree with claims that there is a danger to society, their own rhetorical position encourages them to demand and accept a solution even if that solution involves surveillance measures that contradict their other claims about the loss of privacy rights.

Warrants

The rhetorical grounds expressed by proponents of lawful access legislation used the rhetorical idiom of endangerment and the motifs of old crimes aggravated by new technologies, new crimes aggravated by new technologies, and cyberbullying to rhetorically construct new technologies as a social problem that endangered Canadians. However, the existence of a social problem was not sufficient to authorize government action, despite the grounds that lawful access legislation would address the problem. Claims-makers had to explain why the problem needed to be addressed.

Claims-makers did this by introducing the motif of protection into their rhetoric. Though Ibarra and Kitsuse (1993) more specifically associate the concept of protection with the rhetorical idiom of loss, the protection of Canadians proved to be instrumental to the warrants used to rhetorically construct new technologies as a social problem – and to claims that lawful access was the most effective means to keep Canadians safe. The motif of protection was combined with the motif of obligation, which was used to claim that it was necessary for the

government to respond to the dangers of new technologies, and the motif of childhood vulnerability, which claimed that children were especially vulnerable and entitled to protection.²⁴

Protection Based on Obligation

Within my data, the rhetorical idiom of protection from new technologies was heavily driven by a motif of obligation. The following quotes illustrate the general construction of this rhetoric:²⁵

Nevertheless, sometimes it behooves Parliament to act in a proactive manner and to identify gaps in our law or needed improvements in our law without waiting for mischief to actually take place. In this respect, this is a positive step. (Davies, 2009, p. 6210)

We as parliamentarians have an obligation to protect Canadians and our national interests. The life savings of our citizens, the innocence of our youth, the intellectual property of our research and development sector, our e-commerce and soon even our health records depend on our ability to safeguard that information. (Albas, 2012, p. 5561)

As with the grounds of the claims, claims-makers largely agreed, across the lines established by political parties and in different years, that the government of Canada had an obligation to intervene and protect Canadians from crimes related to new technologies. This motif of obligation was especially important to the rhetoric because it absolved the government of any responsibility with regards to decision-making; because the rhetoric establishes that the government has a moral obligation to act against the problem, it has no choice and cannot be

²⁴ Ibarra and Kitsuse (1993) define a rhetorical idiom of entitlement that “emphasizes the virtue of securing for all persons equal institutional access as well as the unhampered freedom to exercise choice of self-expression” (p. 34). As a rhetorical motif in the context of this research, “entitlement” is instead used to imply that children are especially deserving of additional protections.

²⁵ At the time of their statements, Don Davies was an MP of the New Democratic Party, and Dan Albas was an MP of the Conservative Party of Canada.

considered responsible for its decision or its consequences. Moreover, the above quotes from representatives of the NDP and the Conservative are evidence that there was a broad agreement between political parties that this motif of obligation was a viable moral justification for lawful access legislation.

The rhetorical idiom of protection was also mobilized by law enforcement. Speaking on behalf of the CACP, Jim Chu said that “[the association’s] mandate is the safety and security for all Canadians through innovative police leadership” (Chu, 2014b), invoking the association’s mandate to maintain Canadians’ safety and security. Like political representatives, law enforcement officers claimed that they had an obligation to act and that their actions were necessary to protect Canadians.

To further underline the putative necessity of implementing new lawful access legislation, members of the Conservative government such as MP Ryan Leef also referenced the Convention on Cybercrime (2001):

Finally, it should be noted that Canada is the only G7 country that has not has not yet ratified the Convention on Cybercrime. Further, all countries, including Canada, publicly endorsed the convention for its substantive and procedural framework. It is a model for international co-operation. All of Canada's main partners recognize the convention as a foundation on which international co-operation can be facilitated. (Leef, 2004, p. 8534)

Framed in this context, lawful access legislation was a matter of international obligation: having joined the convention, Canada had an obligation to ratify it and implement lawful access legislation in order to meet its established commitments to international partners. Through this rhetoric, claims-makers who supported lawful access mobilized the Convention on Cybercrime

(2001) as a warrant to reinforce the claims that lawful access legislation was the obligatory solution to social problems such as cyberbullying and cybercrime.

It should also be noted that, despite the rhetorical construction of new technologies as a danger to society by multiple claims-makers, claims-makers showed no willingness to obstruct the technology. As noted above, the claims were that the government needed to update the laws to keep up with new technologies and that it had to protect e-commerce and digital health records. This could have also been achieved by regulating the technology to force *it* to remain within the defined boundaries of Canadian law or to limit e-commerce and digital health records, but instead, the rhetoric focused on adapting the law to the technology and implementing methods of lawful access that would allow the government to use the technology to acquire personal information or intercept communications. In this rhetoric, technological development is inevitable, the government is obligated to protect its citizens, and the only form of regulation available also allows the government to obtain citizens' information through lawful access, thereby expanding the State's surveillance capabilities.

The motif of obligation was further justified by claims-makers who mobilized their own rhetoric about public opinion in order to argue that Canadians expected the government to act. While discussing Bill C-47, Conservative MP Phil McColeman said that "Canadians expect government to protect our children and keep our country safe" (McColeman, 2009, p. 6258), and when supporting Bill C-13, Conservative MP Bob Dechert stated that "[Canadians] want us to protect all people who use the Internet and could be abused by cyberbullies who hide behind the anonymity of the Internet" (Dechert, 2014 p. 6828). During the House committee meetings about Bill C-13, Gregory Gilhooly stated that "victims have rights, and those victims' charter rights deserve to be heard, respected, and considered in the legislation that you are considering at all

times” (Gilhooly, 2014a, p. 11), emphasizing that the government of Canada was acting based on a warrant of obligation and protection in order to guarantee the safety of children and families who – according to claims-makers – demanded government action and were entitled to government protection. It was therefore necessary for the government to act and implement new lawful access legislation regardless of the will of politicians, political parties, or members of government. The rhetorical construction of the warrant denied the possibility that it was an active, deliberate decision. Lawful access was framed as an undeniable *necessity*.

Protection of Vulnerable Children

The primary warrant used to support lawful access legislation based on the grounds that new technologies facilitate or create crime is defined by the motif of protection. As Conservative MP John Carmichael put it, “[w]e worry about our children and young people in an age where technology has clearly moved faster than legislation or regulation” (Carmichael, 2013, p. 1515). This particular quote expresses two important elements of the rhetoric. First, it references the grounds that new technologies are a danger because they are beyond the scope of existing laws²⁶. Second, it specifically associates this danger to “children and young people.” Much like the grounds used cyberbullying to create a more specific sense of dissatisfaction by identifying specific victims of cyberbullying to better highlight the problem – even going so far as to imagine the use of technology in crimes where it was not involved – the rhetoric of protection identifies children and young people as a specific population that needs and deserves the government’s protection. While the motif of obligation insulates the government from the

²⁶ Despite these claims, some laws could still be applied within the context of new technologies. Following the suicide of Rehtaeh Parsons, Segal (2015) published a report on the initial handling of her case by law enforcement. The report notes that “child pornography charges could have been laid at the conclusion of the initial investigation” (Segal, 2015, p. iv), and when the case was reopened, two individuals were charged with and convicted of child pornography charges.

responsibility and consequences of its decision, the motif of children is used to rhetorically construct a vulnerable population that the claims' audience can more easily relate to; government obligation is abstract, but vulnerable children are a tangible and specific rhetorical reality.

Within the rhetorical idiom of protection, the motif of children was used to construct their status as victims – real or imagined. When discussing the relationship between children and new technologies, Senator Pierre-Hughes Boisvenu said that that “[l]orsqu’on donne un outil de cette nature à un enfant de huit, neuf ou dix ans, et qu’on lui permet de l’avoir toute la nuit dans sa chambre à coucher, c’est comme si on donnait la clé de sa chambre à un étranger ou à un pédophile” (Boisvenu, 2014, para. 330) – giving a child access to technology was tantamount to giving a pedophile the key to their bedroom. The empirical validity of this statement is irrelevant next to the rhetorical reality it constructs: children are not safe around new technologies, and giving a child access to new technologies creates the possibility of an imagined crime which, through the claims-making process, becomes indistinguishable from a real crime. In another example of children’s vulnerability, Conservative MP Rob Clarke²⁷ recounted that, while working as a police officer, had seen “how a family was divided and torn apart because their child who had been playing on the computer had formed a conversation with an unknown offender [who] tried to lure that child out of his or her home to meet in a neighbouring community, or in that community itself” (Clarke, 2009, p. 6191). How frequently Clarke encountered such cases, how serious they were, or even whether or not they occurred at all is unimportant. What is important is the rhetoric associated child predators with new technologies

²⁷ The quotes from Boisvenu and Clarke in this paragraph also serve as grounds that new technologies endanger children. They are included in the discussion of the warrant instead so that the analysis can better show the direct link between the motif of children and the motif of protection, and why the government should intervene instead of other institutions such as parents, extended family, or schools. As discussed below, the grounds that children are vulnerable within their own homes disempowers parents and families, and transfers the responsibility for children’s safety to the government. Because of this, the motif of protection is associated specifically with government action.

to construct vulnerable children who are in need of protection, and since the risk – imagined or real – exists within the family home or even the child’s bedroom without the parents being able to keep their child safe, the motif of protection creates a warrant that authorizes the government to protect the children and keep their homes safe in the parents’ stead. New technologies created a fear of crime – which, per Smith and Hill (1991) – can be real or imagined, and the rhetoric uses this fear to implicitly demand action from the Canadian government in its role as formal institution.²⁸

Protection as a Response to the Fear of Crime

The two rhetorical motifs used to supplement the motif of protection – the obligation to act and the vulnerability of children – were used to construct a warrant that could justify lawful access legislation was the ideal solution to the crimes associated with new technologies. To borrow the terminology of Jackson and Gray (2010), the warrant was used to support a *functional* response to the fear of crimes associated with new technologies. Individuals who express functional responses to fear of crime “[take] precautions; these precautions [make] them feel safer; and neither the precautions nor the worries about crime [reduce] the quality of their lives” (Jackson and Gray, 2010, p. 2). The precaution, in this context, is lawful access legislation. Since the claims-makers argue that the government has an obligation to act and that children are unsafe in their homes, the rhetoric presents lawful access legislation as the only solution that can effectively eliminate the risk, reduce the fear of crime, and make children safe.

²⁸ That is to say, the Canadian government’s role as a formal institution within the context of Spector and Kitsuse (1973)’s four stage natural history model of social problems, wherein public groups communicate their claims to the formal institution responsible for the relevant putative social conditions. The key difference here is that the public group is also part of the formal institution. This is discussed later in this chapter.

The ways claims-makers mobilized the motif of protection, the motif of obligation, and the motif of vulnerable children is consistent with broader literature on the relationship between the government and security. In their examination of security, Hagmann, Hegemann and Neal (2018) identify three key dimensions: “the still-powerful historical and conceptual legacy that posits the sovereign state guarantee of ‘security’ as the necessary condition for social, political, and economic life” (p. 9), “a site of contest and political struggle” (p. 9), and “a growing field of governance practices that are increasingly bureaucratized, decentralised, privatised, and technologized, which spill beyond traditional foreign security policy and into the myriad social interactions and economic transactions that permeate globalised life” (p. 9). Each of these dimensions is relevant to my data in some way.

The first dimension, the legacy of the State as a guarantor of security, is most obviously present in the motif of obligation. Claims that the State is obligated to protect citizens and that citizens deserve and welcome the state’s protection reinforce the notion that the providing security is a fundamental responsibility of the State. Meanwhile, the framing of the State as a traditional guarantor of security supports the motif that it is obligated to act in response to the criminal use of new technologies. Thus, the motif of protection and the motif of obligation are situated within the broader context of the perceived relationship of protection between the state and its citizens, and lawful access legislation can be considered part of the State’s security apparatus.

The second dimension, security as a site of political struggle, is noteworthy due to its absence. Much like the common grounds that new technologies posed a danger to society, there was a broad agreement among claims-makers that the motifs of protection, obligation, and childhood vulnerability constituted a valid warrant of action. Liberal Kevin Lamoureux agreed

with proponents of lawful access that “Canadians have little tolerance for cyberbullying and the types of things that take place” (Lamoureaux, 2014, p. 8596), while privacy advocates and critics like Michael Geist agreed that “victims, especially in the cyberbullying context, need to have recourse and need to have appropriate tools” (Geist, 2014a, p. 10). There was no rhetorical opposition to meaningfully question the grounds that new technologies were a danger, that cyberbullying was a danger, that innocent children were especially vulnerable, and that the government had an obligation to respond to the issue. In fact, the motif of protection, as a rhetorical warrant, was even used in a roundabout manner to oppose lawful access legislation, as in the example of NDP MP Jinny Jogindera Sims, who said that “[i]nstead of tackling an issue like cyberbullying and the protection of our children, [the Conservative government] mires legislation with other stuff just so they can have political talking points at a later date” (Sims, 2014, p. 7666), essentially accusing the government of not taking the warrant seriously enough and undermining the protection of Canadians and victims by tying the issue to unrelated policies instead of focusing on the needs of children who were – real or imagined, empirical or potential – of cybercriminals and predators.

Opposition to the claim’s conclusion that lawful access legislation was the best solution to the problem could not refute the warrant based on the motif of protection and attempted to co-opt it and its motifs – particularly that of vulnerable children – to support its counterclaims. There was little political doubt that security was an important concern and that it was the State’s responsibility, and there was little interest in regulating the technologies in ways that did not benefit the State’s surveillance capabilities, even incidentally. The fundamental claim that some measure of lawful access and data interception was widely accepted.

As for the third dimension of security, the bureaucratisation, decentralization, privatisation, and use of technology to extend security concerns to a greater range of government policies, it is seen in the lawful access legislation itself. As a means of surveillance, lawful access creates a bureaucratic structure that decentralizes the surveillance process by spreading it across private telecommunication companies, allowing the government access to their clients' data and integrating surveillance directly into the technology.²⁹ This also situates the surveillance apparatus within the global structure of communication and economic exchanges. Additionally, the motif of protection, as constructed here, extends the State's influence to citizens' homes. By mobilizing the grounds that new technologies allowed predators to contact children inside their homes – or even their bedrooms – claims-makers implicitly established that parents could not protect their vulnerable children, but that the State could do so by regulating the (private) use of technology inside the home through lawful access.

This element of the rhetoric creates an interesting relationship between the State and technology. The rhetoric of endangerment establishes that new technologies pose a criminal danger to society, but the government's use of new technologies is framed by the motif of protection. This creates a dichotomous condition-category that defines non-government use of technology as an inherent danger while the government use of technology is defined as a necessary act of protection; technology is only considered "safe," both to the public and to itself, when it is used under the regulatory framework of lawful access controlled by the state. Though the abuse of government surveillance or the erosion of privacy rights could have similar

²⁹ The Snowden revelations (see Fuchs and Trottier, 2017; Kelly, 2022) provide an example of how this was done in the United States.

consequences to the criminal use of new technologies, these risks are implicitly dismissed because, by rhetorical definition, the government uses the technology to protect Canadians.

Some newspaper coverage provided a more nuanced perspective on the State's relationship with technology. One newspaper article published in 2002 quoted privacy advocates who argued that the government's use of surveillance technologies could also pose a danger to society:

"There's really no need for additional powers to be granted," said Darrell Evans, executive director of the B.C. Freedom of Information and Privacy Association in Vancouver. "Do Canadians really want to create a surveillance society?"

"Are we now saying that technology should be allowed to strip us of our freedoms?" he asked.

Rick Broadhead, an Internet author and consultant in Toronto, said the government is on a slippery slope. If the proposals are implemented in their current form, Canadians may soon see a more restricted model of Internet access, such as that of Singapore or China. (Restivo, 2000, para. 9-11)

Those comments were immediately followed by a statement that "the federal government is merely fulfilling its duties under the Council of Europe's cybercrime treaty, which the government is currently reviewing, according to [Lucie Angers, a spokesperson with the Department of Justice]" (Restivo, 2000, para. 12), so it is unclear what position, if any, the article is meant to convey with regards to the dangers posed by new technologies, and its framing of the government's position is consistent with the motif of obligation that would become prominent in later years.

To summarize, the rhetorical motif of protection integrates the motifs of government obligation and vulnerable children as a response to the endangerment of society by new technologies. This allowed proponents of lawful access to create a rhetorical warrant that other claims-makers neither rejected nor questioned. In the context of the rhetorical motif of protection from technology-related crimes, direct rhetorical opposition did not exist, and when there was some opposition to the government's claims, it attempted to leverage the warrant based on protection rather than the undermine it:

The title is cited as “protecting Canadians from online crime act”, and I have to say at the beginning that I am constantly bothered by the way the government names its bills.

[...]

The immediate issue is important and cannot be lost, so we feel we have to support it, but why do the Conservatives play politics with everything, using cyberbullying to get what they wanted in the old Bill C-30?

[...]

My colleague, the member for Charlottetown, raised a question in the House in which he asked the minister to split the bill, but that was refused. That would have made a lot of sense, in that both aspects of the bill could have been studied in their own right and the cyberbullying aspect of the bill could have been dealt with very rapidly.

This omnibus bill touches upon everything from terrorism to telemarketing to cable stealing to hate speech, and in some parts is an affront to both democracy and the legislative process. (Easter, 2014, p. 8118)

Despite describing Bill C-13 in unflattering terms – “an affront to both democracy and the legislative process” – Easter nonetheless stated that the Liberals felt obligated to support the legislation in order to protect Canadians. Moreover, Easter raised the possibility that lawful access could become a dysfunctional response to the fear of technology-related crime by describing it as a possible affront to democracy and at the very least implying that it could be a cause for anxiety or disrupt Canadians’ lives, but still conceded that the obligation to protect Canadians and victims of cyberbullying, a crime often associated with child victims throughout the rhetoric, was too important to consider the privacy implications of the legislation. Although support for lawful access legislation was neither universal nor unconditional,³⁰ the fundamental premise that the government was obligated to protect citizens was not heavily contested within the rhetoric. The compromise, as referenced by Wayne Easter in the quotes above, would have been to split the bill, separating the uncontroversial measures on cyberbullying and cybercrime from the more controversial surveillance practices of lawful access. According to claims-makers who advocated on behalf of privacy rights, this would have allowed the dangers of new technologies to be addressed promptly while the lawful access itself could have received more thorough debates and consideration, but such opposition still showed some approval for surveillance, as it did not demand that lawful access legislation be abandoned outright.³¹

The Conclusions of the Claim

The grounds that new technologies exacerbate crime by enabling existing crimes or creating entirely new forms of crime establish the foundation of a social problem: new

³⁰ Privacy concerns expressed by various claims-makers are examined in chapter 4 and chapter 5.

³¹ As discussed in chapter 4, members of the opposition parties asserted the grounds that privacy risks and other problems with lawful access legislation could be addressed in committee discussions when Bill C-46 and Bill C-47 were introduced. Suggesting that Bill C-13 should be split so cyberbullying and cybercrime could be debated separately from surveillance follows a similar trend, delaying the discussion of privacy risks and delegating the problem to committees instead of opposing surveillance outright.

technologies endanger Canadian society. The accompanying motifs of children and cyberbullying, combined with specific instances of cyberbullying, serve to define the problem and its causes in specific terms. The rhetorical motif of protection, supported by the motifs of obligation and vulnerable children, build on the grounds to provide moral justification for government action. It is in the conclusion of the claim that this claims-making process fully coalesces in support of lawful access legislation.

When discussing Bill C-13, Conservative Peter MacKay described its consequences as the necessary solution to the problem:

Mr. Speaker, it is a pleasure for me to rise again to take part in this debate on this important legislation. As members opposite would know, the legislation is intended very much to protect people, young people in particular, our most vulnerable; to protect seniors from online criminality and fraud that could defraud them of their life savings; to protect individuals from the security breaches and attacks that we know are happening regularly online. (MacKay, 2014a, p. 8113)

The claim directly states that the purpose of the legislation is to protect Canadians, especially “young people” who are considered “most vulnerable.” Though the quote also refers to older victims and to victims in general, the specific emphasis on young people – children – and the priority they are given in the list raises the rhetorical motif of protection and the motif of vulnerable children, which is made explicit. Simultaneously, references to “online criminality,” “fraud,” “security breaches,” and “attacks” that happen online mobilize the grounds that crimes associated with new technologies. This one quote encompasses much of the rhetoric analyzed throughout this chapter and puts forward its conclusion: lawful access “is intended very much to protect people.” Proponents of lawful access claimed that it was the only solution that solve the

social problem of crimes associated with new technologies, thereby presenting it as a functional reaction to the fear of crime.

The claim that lawful access legislation is the necessary solution to computer-related crimes is implicitly present in police representative Jim Chu's request to the House of Commons:

Give us the tools to help more of these victims, and when we do have a victim, help us to stop the bullying and the harassment early, and stop it from becoming worse, because the worse it gets, the more serious it becomes. Then, of course, it is very traumatic for the victim. (Chu, 2014a, p. 2)

Though this excerpt does not specifically refer to child victims, it does refer to victims in general and specifically mentions bullying. These motifs were used here to claim that law enforcement officials did not have the sufficient "tools" to prevent computer-related crimes and protect victims. Similarly to the way the rhetoric inserted technology into criminal incidents where it was not used and did not exist³² and blurred the distinction between potential crimes and actual crimes to construct crimes associated with new technologies as a dangerous putative social condition, Jim Chu claimed that victims would suffer increasingly serious and traumatic harms if lawful access legislation was not implemented. This claim also served to frame lawful access as a functional response to the fear of crime, as the legislation would address the harm and anxiety caused by the fear of crime and allow police to protect and reassure victims.

Moreover, this part of the rhetoric shows how the claims-making process was used to create a clear distinction between "dangerous" technologies held in the hands of criminals and "protective" technologies used by government representatives. Within the grounds the

³² As is the case with Gregory Gilhooly, who claimed that the predator who groomed and abused him would have used technology to commit his crimes if it had been available at the time, and who was later described as a victim of a cyberpredator by Conservative MP Robert Goguen.

technology itself is framed as a source of dangers: it is the cause of new crimes, it exacerbates some extant crimes, it is related to cyberbullying, it is a problem. The warrant begins to shift the role of the technology by positioning the State as an agent of protection. Thus, when lawful access – and the technology inextricably intertwined with it – is raised in the conclusion of the claim, it is a “tool” necessary to law enforcement and a way to protect Canadians. Though it could be argued that the role of the technology is obfuscated by the role of the legislation, with “lawful access legislation” taking the focus away from the implications of government surveillance, this is also a rhetorical construct that divorces technology from the potential risks of government abuse. Unlike the use of technology by criminals, the State’s use of technology is not associated with endangerment or with the fear of crime.

The culmination of the rhetoric was that renewing lawful access legislation was necessary in order to prevent cyberbullying and cybercrime, and to protect Canadians from the dangers of online spaces and new technologies. Once again, the opposition parties at least partially agreed to the claim and could not challenge its rhetorical premise:³³

Listening to the member speak on the issue of cyberbullying, I was pleased with many of his comments. However, it seems to me that while the government wants to talk a great deal about cyberbullying, if we take a look at the legislation itself, we see that it deals with more issues than just cyberbullying. For example, it was cited in terms of cable theft.

³³ Kevin Lamoureux was an MP of the Liberal Party and Charmaine Borg was an MP of the NDP.

If the government truly wanted to fixate on the issue of cyberbullying and allow for the debate and focus of public attention on that issue, then why would it not just have the bill deal specifically with cyberbullying? (Lamoureux, 2014, p. 4587)

Un autre aspect de la cyberintimidation souligne l'importance d'agir. Avant, l'intimidation se faisait plutôt dans le milieu scolaire, au sein d'un certain groupe d'amis. Toutefois lorsqu'on rentrait chez soi, on était en sécurité, dans une zone sans intimidation. Dans le cas de la cyberintimidation, maintenant que les réseaux sociaux existent, malheureusement, cette zone sans intimidation n'existe plus.

[...]

Le problème, c'est qu'on a malheureusement exclus cet enjeu. Il y a quatre pages sur la cyberintimidation. Qu'a-t-on fait? On a inclus environ 50 pages sur l'accès légal dans un projet de loi sur la cyberintimidation. Il n'y a aucun rapport. (Borg, 2013, p. 1520)

Once again, opposition to the claims did not challenge the grounds that cybercrime, cyberbullying, and other criminal activities related to new technologies created dangerous putative social conditions, nor did they challenge the warrant based on protection used to promote lawful access legislation. Instead, their rhetoric leveraged those same grounds and warrants and used them to conclude that, while lawful access legislation was *necessary*, it was not *sufficient*. The rhetorical opposition was dependent on agreeing with the claim it opposed. This criticism did not seem to pose a problem to representatives of the Conservative government, who claimed that, while lawful access was a key component of their approach to technology-related crimes, it was still only one component among others:

Mr. Speaker, what we have with Bill C-13 is a comprehensive bill that would get the job done. It is also important to recognize that not only do we have the bill in front of us here, but we have many other measures. We talk about the need for prevention. We talk about the need for education. This is one piece of an important puzzle, but what this piece of legislation would do is be comprehensive in terms of how it would tackle this issue in an effective way. (MacLeod, 2014, p. 8537)

Thus, opposing claims-makers were consistently unable – or unwilling – to rhetorically challenge the principal grounds, warrants, or conclusions of the government and other proponents of lawful access.³⁴ This was explicitly stated by Wayne Easter during debates about Bill C-13:

The bill was not split. However, regardless, we do feel within the Liberal Party that cyberbullying is such a scourge on society that we are going to have to put not only a little water in our wine, but a fair bit, in fact, because we are very seriously troubled over aspects of the bill. (Easter, 2014b, p. 8531)

Wayne Easter expressed regret that the legislation was not split,³⁵ which would have allowed the social problems of cyberbullying and surveillance to be discussed separately, and clearly stated that supporting the legislation was undesirable to the Liberal Party, yet the Liberals nonetheless

³⁴ Different social problems associated with lawful access legislation faced varying degrees of opposition and different rhetorical strategies, which are discussed in other chapters. This point of analysis applies specifically to the rhetoric of endangerment from cybercrime, cyberbullying, and other crimes associated with new technologies.

³⁵ The claim that the legislation should have been split to separate the issues cyberbullying and cybercrime from surveillance could also be addressed in Chapter 4, which examines claims that lawful access legislation would result in a loss of privacy rights. It is brought into focus in this chapter instead because it is fundamentally based on the rhetorical idiom of endangerment; on the grounds that cyberbullying is a danger to Canadian society and the warrant that Canadians must be protected, it is claimed that the legislation should be split so that the threat of cyberbullying can be addressed quickly.

concluded that supporting the legislation was necessary because cyberbullying – and by extension, crimes related to new technologies – was too great a danger to Canadian society.

The Liberal Party’s claim can be interpreted through the counter rhetorical strategy of the costs involved:

The upshot of this technique is to say that the problematic condition-category must be lived with rather than remedied through the claimant's specific measures, either because “two wrongs don't make a right,” or because the claimed “benefits” do not outweigh their “costs.” (Ibarra and Kitsuse, 1993, p. 39)

In this instance, the Liberal Party claimed that the benefits of protecting privacy rights did not outweigh the costs of delaying legislation on cyberbullying because cyberbullying was too great a threat to Canadian society. As a result, the Liberals claimed they were compelled to support the legislation in spite of their objections.

This provides a concrete example of how security is prioritized over privacy rights. According to Bannister (2005), is often treated as something to be traded in exchange for something else, such as laws on cyberbullying. Counter rhetorical strategies are “are discursive strategies for countering characterizations made by claimants” (Ibarra and Kitsuse, 1993, p. 30). In this case, the Liberal Party made a counterclaim against its own rhetorical position, countering their characterization of lawful access legislation as an unacceptable loss of privacy rights³⁶ and undermining their own claims.

This in turn raises the question of how fear of crime is managed and used to guide rhetoric and policy. Jackson and Gray’s (2010) study of reactions to the fear of crime used a

³⁶ The specific claims that lawful access legislation would result in a loss of privacy rights are examined in Chapter 4.

three-step process to determine if an individual's reaction to the fear of crime should be considered functional or dysfunctional:

- First, measure worry about crime using standard intensity measures (e.g. 'How worried are you about being burgled?': very, fairly, not very, not at all);
- Second, if individuals who say they are fairly or very worried also report that their quality of life is reduced by either their worries or their precautions against crime, then assign these individuals to the dysfunctionally worried group; and
- Third, if individuals who say they are fairly or very worried also report that they take precautions that make them feel safer, and neither worry nor precaution reduces their quality of life, then assign these individuals to the functionally worried group. (Jackson and Gray, 2010, p. 5)

Since Wayne Easter described cyberbullying as a “scourge,” it is reasonable to conclude that the Liberals expressed they were “very” or “fairly” worried about crime. “Quality of life” is more difficult to evaluate with this data, but given that the Liberals were “very seriously troubled” about Bill C-13’s privacy implications, it is also reasonable to conclude that the party’s support for the legislation represented something analogous to a dysfunctional reaction to the fear of crime.

Situating this rhetoric within the broader field of research on security and privacy, the problem is not only that proponents of lawful access legislation garnered support for their policies by citing threats to society, as is often the case (see Akdeniz, 2002; Etter, 2001; Lyon, 2003; Mathiesen, 2013; Pallaras, 2011), but that some claims-makers who expressed resistance or opposition to the legislation on the grounds of its privacy implications chose to support it over their own objections. Security threats do not command unconditional support, but as Bannister

(2005) notes, privacy is often treated as something to be exchanged for something else, whereas there is little to no apparent willingness to accept some measure of danger to prioritize privacy rights instead.

It is also particularly noteworthy that Carol Todd also expressed concerns about the privacy implications of Bill C-13 and implied that the surveillance measures should be excluded from the bill:

Bill C-13's cyberbullying provisions are needed for my wish to come true as a mother of a cyberbullying victim. While I applaud the efforts of all of you in crafting the sextortion, revenge porn, and cyberbullying sections of Bill C-13, I am concerned about some of the other unrelated provisions that have been added to the bill in the name of Amanda, Rehtaeh, and all of the children lost to cyberbullying attacks.

I don't want to see our children victimized again by losing privacy rights. I am troubled by some of these provisions condoning the sharing of the privacy information of Canadians without proper legal process. We are Canadians with strong civil rights and values. A warrant should be required before any Canadian's personal information is turned over to anyone, including government authorities. (Todd, 2014, p. 2)

Carol Todd's testimony is significant because, according to Spector and Kitsuse's (1973) four stage natural history model, social problems emerge when public groups in society make claims about putative social conditions they deem problematic. In the case of lawful access legislation, however, Carol Todd's testimony occurred several years after the Conservative government began to make claims about cybersecurity and lawful access, which changes the expected relationship between claims-makers. Rather than take up claims made by relatives of victims of cyberbullying, the government integrated their claims into its own. Moreover, the Conservative

government interpreted Carol Todd's claims in a manner that supported lawful access legislation, despite her explicit support for privacy rights:

I wonder if the member heard that Ms. Todd met with the Minister of Justice following her appearance at the justice committee and then did a subsequent CBC Radio interview about two or three days later. I wonder if the member heard that interview and what she said then. Maybe he could quote from that next time he has an opportunity. If he has not had a chance to hear that interview, I would be happy to provide him with a transcript. He would find that after speaking with the Minister of Justice, Ms. Todd understood why many of these investigative powers are necessary in order to prevent the kind of thing that happened to her daughter from happening again. (Dechert, 2014, p. 7662)

The grounds Carol Todd used to express support for Bill C-13 were emphasized, while the grounds she cited to express opposition to the legislation were negated and dismissed. This demonstrates how the state can use claims made by members of the public to support its own policies. In this instance, Carol Todd clearly claimed that cyberbullying was a social, but her claims did not include the investigative powers and their privacy implications. Those aspects of that legislation were reinforced by the government (partially) on the grounds of Carol Todd's own claims in order to garner support for Bill C-13.

Chapter 4: Loss of Privacy, Part 1

Privacy rights are a key issue in any discussion of surveillance. Lyon (2003), Andrejevic (2007), and Mathiesen (2013) all warn that state surveillance can expand the power of the state and undermine citizens' privacy rights, rights that are necessary to democracy. As Mladenov and Galetin (2025) put it, “the right to freedom of expression is contingent upon the right to confidential communication” (p. 581), and although their research focuses more specifically on encryption, the same principle can apply to the confidentiality of communication in general. This is especially true in the context of social media, which has become a common medium of political activity (Hong and Kim, 2021; Pandey, Gupta, and Chattopadhyay, 2020), as it exposes users to incidental political news (Scheffauer, Goyanes, and Gil de Zúñiga, 2021), allows protest groups to mobilize and attract attention to their cause (Schaaf and Quiring, 2023), provides easy access to public feedback and engagement (Velasquez and LaRose, 2015), and creates new digital spaces where youth can engage in political activism outside the control of authoritarian regimes (Godfrey and Simbarashe, 2025). Furthermore, Pandey, Gupta, and Chattopadhyay (2020) note that the internet allows people to participate in political activities anonymously if they so choose, highlighting the importance of privacy to political speech.

State surveillance can sometimes conflict with political activities that rely on digital communications. In the field of journalism, Lashmar (2016) and Brevini (2017) argue that communication metadata³⁷ collected by the state could be used to identify journalists' sources, which would undermine the integrity and freedom of the press, and Smyth (2012) discusses the chilling effects of law enforcement agencies collaborating with private companies and civilians

³⁷ Lashmar (2016) defines metadata as “information that accompanies and individually defines emails, phone calls, texts and other electronic communications but is not the content data” (p. 683).

to gather evidence from the internet and social media. More directly, political activism is often equated with terrorism or other public security threats that are vaguely defined (Crosby and Monaghan, 2016; Lyon, 2003; Mathiesen, 2013; Monaghan and Walby, 2012; Proulx, 2014), and surveillance measures often perpetuate various forms of discrimination (see Hanniman, 2008; Jamil, 2017; Nagra and Maurutto, 2016; Smith, 2009). There is also a risk that *judicial* expectations of privacy expectations and *personal* expectations of privacy expectations will not align (Crowther, 2012), which can potentially expose individuals to criminal investigations based on communications, actions, or other forms of evidence they considered private, but that were considered legally accessible by law enforcement agencies.

The literature is rife with examples demonstrating both that political activists are interested in using modern telecommunications technologies for political purposes and that the state is interested in obtaining these communications through measures such as lawful access, which risks undermining privacy rights and, by extension, democratic rights necessary to political activity. Accordingly, privacy risks sit at the centre of the discussions around lawful access. This chapter examines these risks through the rhetorical idiom of loss, which emphasizes “loss of prestige or value accorded to [a] sacred object” (Ibarra and Kitsuse, 1993, p. 37). In the context of lawful access legislation, claims-makers applied the rhetoric of loss to privacy rights which, according to them and their claims-making activities, were devalued in favour of security and surveillance.

This chapter shows how some claims-makers rhetorically constructed lawful access legislation as a social problem because it would, according to them, result in a loss of Canadians’ democratic privacy rights. The grounds of this claim were based on the rhetorical motifs of privacy as an inherently important civil right, the putative absence of sufficient oversight

measures in the legislation, and the divisions established by political partisanship. To justify their claims and assert the importance of privacy rights, claims-makers mobilized rhetorical warrants based on the motifs of the balance of security and privacy and of the importance of democratic rights. Through these motifs, claims-makers who defended privacy rights in response to lawful access legislation constructed their claims that the legislation would erode privacy rights and therefore should be considered a social problem.

Grounds

To study the claims-making activities that constructed the loss of privacy as a putative social problem, it is first necessary to examine the grounds established by claims-makers. Because grounds are statements of fact used to establish the rhetorical truth of the claim (see Best, 1987; Toulmin, Rieke and Janik, 1984), they contain, within the context of this chapter, the evidence presented by claims-makers that lawful access legislation would result in a loss of privacy rights. As discussed in this section of the chapter, three major rhetorical motifs emerged from my data to categorize the grounds of the loss of privacy: the importance of privacy as an inherent civil right, the absence of sufficient oversight measures to ensure lawful access legislation and its related surveillance measures would not be abused, and political partisanship, which was mobilized in the claims-making process by politicians to advocate for their political party's policies.

Privacy and Democratic Civil Rights

To establish the importance of privacy rights, privacy advocates mobilized grounds that described the legal and political implications of privacy as an inherent civil right. This rhetorical approach focused on the importance of privacy itself and on the established the need for privacy rights in the democratic relationship between the state and the citizens who, at times, need to be

protected from the state's interference in their personal lives. According to these grounds, the loss of privacy becomes a social problem not only when it has negative consequences, but at the very moment privacy rights are infringed upon. Michael Spratt and Marian Brown, two representatives of the Criminal Lawyers' Association, discussed this issue when they testified to their importance before the Standing Committee on Justice and Human Rights during Bill C-13:

What's the danger with people asking for this information? I'm sure you've all read the stories about record checks, police checks, state storage of information, disclosure of that information. That's the danger. It's not an answer to say that if you have nothing to hide, you should be willing to give this information over. What's the harm? The harm is done when the charter is breached. That's the standard. The tie doesn't go to the victim. The tie should go to the charter, which is the supreme law and should be respected. (Spratt, 2014, p. 10)

Yes, infringement of a charter protected privacy interest is a harm. Privacy is something that we value in our justice system and to infringe someone's privacy in those circumstances weakens the protection of everyone's privacy in general. (Brown, 2014, p. 9)

These grounds describe privacy rights as inherently important. According to Spratt and Brown, the loss of privacy rights does not occur when individuals curtail their political activities out of fear or when they are unfairly discriminated against or criminalized. The loss of privacy rights occurs when the privacy rights are breached and the State enters a personal space that it should not have access to, regardless of the consequences. As such, privacy rights are important not because of how they affect individuals who are placed under surveillance for one reason or another, but because of the fundamental legal protection they provide to Canadians. The loss of

privacy rights is caused by neither tangible harms nor visible consequences, but by an infringement of charter rights that undermines the political and relationship between the democratic state and its citizens.

Further emphasizing the possible risks posed by the expansion of surveillance measures, Privacy Commissioner of Canada Daniel Therrien raised concerns about the number and types of agencies that would be able to obtain information through lawful access while testifying about Bill C-13 in 2014:

A second concern is the broad range of authorities that can rely on these powers. The investigative powers and provisions in Bill C-13 see both peace officers and public officers at all levels of jurisdiction in Canada broadly empowered with a whole range of new techniques. While many law enforcement and security agencies have robust accountability mechanisms, other government bodies implicated by this definition have no dedicated review and no transparency requirements. We find this to be of particular concern. (Therrien, 2014, p. 2)

Additionally, Therrien also argued that Bill C-13 should maintain higher standards – “reason to believe” rather than “reason to suspect” – before authorizing requests for information rather than making personal information easier to obtain:

We believe that suspicion is too low a threshold for such potentially revealing information in a digital era, when every transaction, every message, every online search, and every call or movement leaves a recorded trace. As a result we suggest the bill use the traditional standard of reasonable and probable grounds to believe for the provisions under which access to information would be granted. This is the standard that should hold

until a more compelling case for the use of a reduced legal threshold is presented and thoroughly examined. (Therrien, 2014, p. 2)

Thus, Therrien addressed the risk that Bill C-13 would allow information to be obtained by multiple parties held to different standards of oversight, that the information requested could reveal very private information, and that the threshold to request information would too low to respect privacy rights. Combined, these putative facts serve as grounds to claim that the legislation would indeed constitute a significant loss of privacy rights.³⁸

The grounds used to define the scope of surveillance also reflect its political implications. Privacy advocate Michael Geist, Canada Research Chair of Internet and E-commerce Law at the University of Ottawa, testified that “we know that at least 750,000 Canadian user accounts are voluntarily disclosed every year—one every 27 seconds” (Geist, 2014a, p. 7), which shows how often personal information is disclosed and how precarious privacy rights are. Moreover, claim-makers raised concerns about the content of the information being disclosed. Associate Professor Andrea Slane of the University of Ontario Institute of Technology said that the information collected included “your transactions with all the social media sites, plus the places where you browse, things you are taking a look at, people you call, things you are inquire about” (Slane,

³⁸ Additionally, privacy commissioners and police representatives debated the privacy implications of Bill C-30 in an exchange of news articles. Elizabeth Denham was the information and privacy commissioner of British Columbia, Ann Cavoukian was the information and privacy commissioner of Ontario, and Jill Clayton was the information and privacy commissioner of Alberta. On November 5th, 2012, Jim Chu, Chief Constable of the Vancouver Police Department, (Chu, 2012c) published a newspaper article on behalf of the CACP in order to defend Bill C-30. The privacy commissioners published a joint newspaper response on November 7th (Clayton, Denham, and Cavoukian, 2012), with Jennifer Stoddart, the privacy commissioner of Canada, also publishing a response on November 8th (Stoddart, 2012b). This led to Jim Chu publishing another defense of Bill C-30 on November 10th (Jim Chu, 2012b), specifically replying to the privacy commissioners, who then published another response to Jim Chu on November 14th (Denham, Cavoukian, and Clayton, 2012) and November 15th (Stoddart, 2012a). Ann Cavoukian published another article on December 3rd (Cavoukian, 2012b), which Jim Chu then responded to on December 6th (Chu, 2012a). Ann Cavoukian responded once more on December 7th (Cavoukian, 2012a). The opinions published by Jim Chu reflected the rhetoric of proponents of lawful access, while the opinions of the privacy commissioners reflected the rhetoric of privacy advocates. These exchanges are specifically highlighted here to provide additional context for the privacy commissioners’ statement and because this was the only instance of officials debating lawful access in the newspapers that I could find in my data.

2014, para. 261) and argued that when this information was combined, the result was “more invasive than what one social media company gets” (Slane, 2014, para. 261), emphasizing the broader implications of increasingly widespread surveillance. Though any amount of disclosure would, as discussed previously, constitute a loss of privacy rights according to privacy advocates, the increased frequency of information requests increase the risk that information gathered from multiple relatively “minor” privacy violations could be combined to obtain – or perhaps deduce – even more important personal information, which would lead to a more severe privacy violation and a greater loss of privacy rights that are, according to claims-makers, necessary to protect citizens. Similarly, Bailey’s (2008) analysis of the different legal privacy standards applied to the physical body, the home, and personal information suggests that, because modern telecommunication technologies are so widespread, personal information can now reveal more sensitive details that could not be captured in the past, and Lessig (1999a; 1999b) raises concerns about the data collection integrated directly into modern technologies and how discrepancies between older – and potentially outdated – legal standards of privacy and the way modern technology is used can further erode privacy rights. Furthermore, Haggerty and Ericson’s (2000) study of the surveillant assemblage suggests that modern surveillance is driven by “the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole” (p. 610), much like the privacy commissioners’ concerns that information collected from multiple sources could be combined to create more detailed profiles that would constitute a violation of personal privacy. Thus, the putative social conditions presented by claims-makers who were concerned about the loss of privacy – the importance of privacy as an inherent legal and democratic right and the ways in which widespread data collection make personal information and communications increasingly sensitive because of the picture they paint when

collated – reflect broader discussions within the field of privacy and provide a basis for the claim that the loss of privacy caused by lawful access legislation is a social problem.

The rhetoric expressed by claims-makers who were members of the House of Commons' opposition parties was more nuanced, but they also generally agreed with the grounds that the loss of privacy rights due to lawful access would be a social problem for Canada. As NDP MP Jack Harris put it:

When the state desires to interfere with that privacy and to carry out a search or surveillance of these communications, under our law there is a requirement that there be judicial oversight to provide a warrant in most cases, unless someone is caught in the act. No one can enter a person's house, for example, without a warrant, unless under hot pursuit of someone who has just committed a crime.

There are protections for fundamental freedoms and legal rights, including the right to be secure against unreasonable search and seizure. These are the kinds of fundamental rights that we have in our society. (Harris, 2012, p. 5594)

Like privacy advocates, Jack Harris identified privacy as a “fundamental” legal right necessary to protect the public from unreasonable search and seizure and other state abuses. Similar to Michael Spratt and Marian Brown, Jack Harris situated the loss of privacy not solely in the consequences of the privacy breach, but within the privacy breach itself. This further reinforces the grounds that privacy rights and privacy protections are necessary political and democratic rights. Thus, the infringement of privacy rights is, according to some claims-makers, sufficient to claim that the loss of privacy is a social problem because it is evidence that the state does not want to respect citizens' legal rights.

Nevertheless, the consequences of privacy breaches – including, as discussed previously in this chapter, the collection of information by various government agencies for purposes that are not necessarily relevant to criminal investigations, the high frequency of information requests, and the ability to combine information from multiple sources to obtain more personal profiles – are valuable grounds because they describe the loss of privacy as a social problem in more specific and concrete terms. From this perspective, claims-makers developed grounds that information obtained through lawful access could lead to broader privacy violations, thereby exacerbating the loss of privacy. As Liberal MP Judy Sgro put it:

Giving the police and government the right to warrantless searches of private emails and web-browsing activity is conceptually the same as allowing police to view bank records, to monitor private mail and to snoop into the most private elements of a person's life for no particular reason. I cannot imagine that anyone in this House on any side would want that to happen. (Sgro, 2012, p. 5592)

These comments recognize that private information that does not seem *too* private – emails and web-browsing activities – can potentially reveal much more personal information such as bank records or other information that should be considered private, echoing, like Slane, the privacy risks raised by Lessig (1999a; 1999b). Though lawful access may target telecommunication technologies that are not considered to be highly private – see for example Bailey's (2008) pyramid of early judicial decisions that position informational privacy as less problematic than bodily or territorial privacy – the information communicated through these technologies can have much more important privacy implications. This is precisely the argument that the Supreme Court of Canada adopted in its shift away from simplistic analyses of information in *R. v.*

Spencer (2014). Again, the power of democratic governances both as a ground and as a rhetoric places privacy firmly in the centre of democratic governance relationships.

The importance of the democratic relationship between the state and its citizens was also raised by the inclusion of the Snowden revelation in the rhetorical discussion of Bill C-13. NDP MP Wayne Marster referred to Snowden to provide additional grounds that surveillance practices were a widespread problem and that privacy rights were being infringed upon on a large scale:

Mr. Speaker, I would like to offer one word in the beginning of my remarks, which is Snowden. 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. (Marster, 2014, p. 7668)

For context, 2013, Edward Snowden was a contractor working for the National Security Agency (NSA) who, in 2013, leaked information about the NSA's surveillance infrastructure to journalists (Byman and Wittes, 2014; Weinstein, 2014). These documents revealed that the American government was regularly spying on its citizens (Byman and Wittes, 2014; Finley and Esposito, 2014) and caused several international scandals (Finley and Esposito, 2014). These revelations occurred after Bill C-30, but overlapped with Bill C-13 and thus became part of the rhetorical claims-making process.

As a rhetorical motif, the Snowden revelations carry both explicit and implicit meanings. The above quote from Wayne Marster carries the explicit meaning of the revelations as grounds that demonstrate the loss of privacy: “improper access” of metadata, “thousands upon thousands of examples” of wrongdoing and unlawful surveillance, metadata “abused and put into the wrong hands.” Snowden gave the opposition parties specific, concrete, and widely-publicized grounds to claim that government surveillance could be abused. Misuse of government surveillance,

unlawful surveillance, and breaches of privacy were no longer a hypothetical reality. They became something that *had* happened and that *could* happen again, which allowed the claim-makers to define the putative loss of privacy through more specific grounds.

The implicit meaning emerges when the Snowden revelations are examined through the broader context of academic research. Austin (2015) describes the NSA's surveillance measures as a “lawful illegality” (p. 103), a term which is derived from “conflict between the perspective of the state and the perspective of ordinary citizens” (p. 103). When lawful illegality takes place within the context of surveillance, ordinary citizens believe that broad surveillance measures *must* be illegal, while the state argues that its surveillance measures are perfectly legal, leading to conflicting interpretations of the law and of privacy rights. Michael Geist touched on this topic while testifying before the Senate:³⁹

I wasn't aware of that case. I'm tempted to say maybe that's why there's a third edition.

In a sense, we're talking there about two different things. We're talking closer to what Senator Frum was talking about and what the average user feels about the kind of privacy they have when they engage in online activity. I think it is the case that for a lot of users, and certainly in a post-Snowden environment, that's accurate. We learned through Snowden, in a world in which security intelligence agencies are hoovering up all of that information, that the notion that somehow those emails are private is wrong. That just doesn't happen.

³⁹ This quote was a response to a question by Conservative Senator George Baker about *Internet Law in Canada*, which was written by Michael Geist (2001). A passage of the book states that e-mails are neither private nor secure because they are accessible to ISP staff as well as their intended recipients. Senator George Baker asked Michael Geist if those comments were still relevant.

But that's not really what is at stake or at issue here. At issue isn't whether or not emails themselves can get captured in a myriad of different ways unless you take steps to encrypt them to provide some level of privacy over those messages. The issue is the standards that we establish in terms of when law enforcement can obtain that under a search and then use that information. That's something quite different. (Geist, 2014b, para. 287-289)

This testimony referenced the putative gap between citizens' expectations – “what the average user feels about the kind of privacy they have when they engage in online activity – and the reality of “security intelligence agencies [...] hoovering up all of that information” which individuals consider private to establish the grounds that there was a fundamental misunderstanding between citizens and the state with regards to privacy rights, with citizens expecting their information to remain private while the state expected it to be available at its convenience. Thus, through the perspective of lawful illegality – a putative social condition that could be considered a social problem due to the conflict between the state and its citizens – the rhetorical motif of the Snowden revelations are grounds to conclude that lawful access legislation results in a loss of privacy because citizens and the state hold privacy rights to different standards and possess different understandings of privacy as a necessary political and democratic right that is meant to protect citizens from illegal state surveillance.

Though the analysis above focuses on Bill C-30 and Bill C13, my data also show that the loss of privacy was a concern during the rhetorical construction of previous bills. Bloc Québécois MP Guy André emphasized, while discussing Bill C-46, that information obtained through lawful access had privacy implications and should be handled carefully:

En effet, ces nouveaux moyens d'enquête conférés à la police permettent un accès à un très grand nombre d'informations. Ces informations doivent évidemment être traitées tout en protégeant la vie privée des citoyens. Surveiller les agissements de quelqu'un dans l'Internet permet d'en savoir beaucoup plus sur sa vie privée. C'est cela, notre mise en garde. (André, 2009, p. 6215)

Liberal MP Mark Holland stated that lawful access could lead to abuses or malicious breaches of privacy:

A number of people have expressed concerns that a law of this nature could be misused to allow access into people's searching history and people's personal messages or could be used maliciously by somebody to gain access to people's Internet search records and history. (Holland, 2009a, p. 6181)

And NDP MP Joe Comartin discussed the links between new technologies and private communications, arguing that they should not be available without a warrant:

However, in the course of that debate in the country and in, I will say, the high tech community in this country, there was great concern expressed about privacy rights and about the role the state should play in getting access to private communication and private data. I think there was a general consensus in the country, and in those communities that were particularly interested in this area, that that should never be done without a warrant. (Comartin, 2009, p. 6321)

In short, claims-makers who were members of official political parties and who formed the political opposition to the Conservative government were aware of the importance of privacy rights and were also aware that lawful access could cause a putative loss of privacy.⁴⁰

The grounds discussed in this section demonstrate how, according to claims-makers who advocated for privacy rights, lawful access legislation risked infringing upon privacy rights, and this infringement would constitute a harmful loss of privacy the moment it occurred. In this context, the other grounds cited by claims-makers, such as the Snowden revelations, evidence of frequent demands for personal information, the possibility that more detailed personal profiles could be assembled by obtaining information from a wide variety of sources, and the possibility that the state could gain access to personal information without a warrant, serve the rhetorically emphasize the risks of lawful access by showing how a “minor” infringement of privacy rights could allow the state to obtain a significant amount of personal information about an individual; the harms caused by such an intrusion exacerbate the harms caused by the initial breach of privacy. Thus, the loss of privacy can be considered a social problem because it allows the state to enter into the personal space of its citizens – a space it is not meant to be enter arbitrarily in a democratic society – and obtain information that should be considered private. The concerns claims-makers raised about warrants – or lack thereof – is further evidence of this, as warrants are a legal mechanism meant to ensure that that the state cannot intrude upon citizens’ private matters. This leads to the discussion of oversight, another rhetorical motif critical to the grounds of the loss of privacy.

⁴⁰ Though members of the opposition parties recognized that lawful access legislation could result in a loss of privacy rights, they also agreed that new technologies were a danger to Canadian society and that lawful access legislation was necessary to address these dangers (see chapter 3).

Privacy and Oversight

In addition to expressing concerns about the infringement of privacy rights and the misuse of lawful access, claims-makers also found grounds to be concerned about the process used to make information requests and what it implied for the democratic relation between the state and its citizens; the putative lack of strong oversight measures was considered a problem that would exacerbate the loss of privacy because it would make it difficult, if not outright impossible, to determine if and when privacy rights were infringed upon, how the damage caused should be repaired, and how future infringements should be prevented, all as a result of the state's exercise of surveillance power. This could further erode the democratic principles that support privacy rights.

Scholars such as Moore (2011) and Nyst (2018) agree that proper oversight of state surveillance is necessary to privacy, and that privacy plays a key role in democratic governance, and many claims-makers expressed similar sentiments with regards to lawful access legislation, particularly for Bill C-13 and Bill C-30. Stephen Anderson, the Executive President of OpenMedia.ca, testified that “Bill C-13 [did] not, in its current form, provide effective measures to increase transparency, accountability, or reporting on warrantless access to private data” (Anderson, 2014, p. 6) and that the “proposed lowering of the 'reason to suspect' threshold for transition data warrants [was] also of concern to Canadians” (Anderson, 2014, p. 6), claiming that the loss of privacy rights was not simply an abstract legal matter, but a matter of importance to Canadian citizens and their personal interests – an example of how claims-makers rhetorically positioned privacy within the broader contexts of public interest and of the democratic relationship between the state and its citizens. By mentioning “transparency, accountability, [and] reporting” as rhetorical motifs, Stephen Anderson addressed important elements of democratic

society that allow the citizens to be aware of the state's actions and hold the state accountable for them. Moreover, mobilizing the grounds that the lowered threshold for transition data warrants was “of concern to Canadians”⁴¹ invokes public opinion to provide grounds that privacy, as a political right, was important to Canadians and that they expected their privacy to be respected and protected.

Speaking of the oversight following an information request, privacy advocate David Fraser noted that there was “no mechanism in these for notifying the individual after the fact that their information has been accessed” (Fraser, 2014, p. 2), which would leave individuals unaware of any privacy rights violations they suffered, and since, as discussed previously, the harms of privacy violation are inherent to the breach of privacy rights, the putative absence or insufficiency of a notification mechanism would, according to claims-makers such as David Fraser, make it impossible for individuals to seek compensation for the loss of their privacy rights or for citizens as a whole to hold state to account for abuse of power; indeed, these grounds suggest that the individuals placed under illegitimate surveillance would never be informed that their rights were violated, leaving them ignorant to the fact that they lost some of their of privacy rights and eroding the general principle of democratic transparency. This would, in turn, make it much more difficult – if not impossible – to hold the state and law enforcement agencies accountable when they exercise their powers in ways that infringe upon privacy rights.

Further highlighting the importance of collaboration between the state and telecommunication companies – a collaboration that was also revealed by the Snowden revelations discussed previously – Bill C-13 also included a provision that granted immunity

⁴¹ Per social problem theory, grounds are fact if they are presented as facts by the claims-makers. In the context of the rhetoric, there is no need to provide specific empirical evidence that Canadians were concerned about the threshold police had to meet to request data.

from civil liabilities to parties that cooperated with a request for information made through lawful access. Feminist advocate Steph Guthrie described the provision thusly:

One of the most troubling provisions in Bill C-30 was that it mandated the disclosure of user information to police without a search warrant. The newly designed provision in Bill C-13 very cleverly softens this, instead stating that police can request information, and the person or organization to whom they direct their request can voluntarily comply. However, the very next provision in Bill C-13 removes all civil liability for anyone who discloses another person's information to police upon request. This granting of immunity removes much of the incentive for an Internet service provider, or anyone else, to deny the request. (Guthrie, 2014, p. 6)

According to these grounds, the fact that the immunity from civil liability “removes much of the incentive for an Internet service provider [...] to deny the request” would, in practice, amount to warrantless surveillance.⁴² By discursively raising the motif of warrantless surveillance, Steph Guthrie established grounds that the state would be allowed to request information from service providers without the constraints a warrant would provide, thereby allowing the state to essentially obtain information about any individual at its convenience, and individuals whose privacy rights were infringed upon would not be able to hold service providers liable for their breach of trust. Steph Guthrie’s rhetoric constructs an image of the state that prioritizes surveillance and information-gathering at the expense of privacy rights, exempts itself from democratic checks and balances normally enforced by warrants, and removes any obstacles that might discourage other parties from sharing personal information they might possess. Not only

⁴² That Bill C-13 held lawful access requests to the threshold of “reason to suspect” instead of the more stringent “reason to believe” is further grounds to claim that lawful access legislation weakened the importance of warrants as measures of legal oversight and accountability meant to ensure the state would not abuse its surveillance powers.

does this rhetoric provide grounds that lawful access would result in a loss of privacy rights, it also provides evidence that citizens would have little to no recourse if their rights were infringed.

Following the same rhetoric, Liberal Sean Casey also compared Bill C-13 to warrantless surveillance:

Clause 20 of the bill, specifically proposed section 487.0195, addresses voluntary disclosure of information by, for example, telecommunications companies and Internet service providers. In a circumstance in which electronic information is voluntarily disclosed, they are given absolute immunity. Therefore, in a case where there is a co-operating party, there is indeed no judicial oversight and no sanction. In fact, there is immunity given. It is really not far from a warrantless search when we have a willing party holding the data. That, in our view, is the poison pill in this legislation. (Casey, 2013, p. 1439)

The comparison between providing immunity for voluntary disclosures of information and warrantless surveillance establishes the grounds that lawful access legislation would allow the Canadian government and law enforcement agencies to obtain information without the judicial oversight that normally determines whether or not a search or request for information should be considered legal according to Charter rights and established privacy standards. According to the rhetoric of Sean Casey and other claims-makers who supported privacy rights, allowing telecommunication companies to share information with law enforcement without fear of negative legal repercussions or liabilities would be functionally identical to warrantless surveillance. In this way, the rhetoric collapses lawful access into the motif of warrantless search, creating a strong implication that lawful access legislation would be responsible for the loss of privacy and the associated mechanisms of accountability, transparency, oversight, and

compensation. Therefore, the rhetoric constructs a social reality wherein citizens are under the constant threat of state surveillance which is invisible to them and which they cannot really contest because the democratic institutions that would allow such a contest – warrants, oversight, civil recourse, and a commitment to privacy rights from both the state and private parties – no longer exist.

The rhetorical strength of warrantless surveillance as a motif is further amplified by the rhetorical motif of oversight, which integrates democratic principles of accountability and constraints on state power into the rhetoric. The motif of oversight was adopted by many claim-makers among the political parties; in one instance, Rosane Doré Lefebvre, an MP of the NDP, outlined some of these issues, linking them to Conservative governance and to international surveillance and investigations:

À la Chambre, nous avons posé beaucoup de questions à ce sujet. Nous avons besoin d'avoir un mécanisme de surveillance. Depuis que les conservateurs sont au pouvoir, il n'y a jamais eu autant de demandes d'utilisation de renseignements personnels. Or, il n'y a aucun mécanisme de surveillance qui nous permette de faire état de ce qui se passe et de voir de quelle façon nos données sont utilisées. Ces données ne sont pas utilisées seulement à l'intérieur du Canada; elles sont partagées avec différents corps de police ainsi qu'avec différents organismes internationaux. C'est inquiétant pour la vie privée. (Lefebvre, 2014, p. 10)

The increase in information requests – specifically associated with the Conservative Party rather than the government as a whole, which paints the Conservatives as anti-privacy and anti-democratic while positioning the NDP as the protectors of Canadians' democratic privacy rights, though they themselves also mobilized security grounds to advance lawful access at times – and

the sharing of private information with international law enforcement organizations was grounds to claim that lawful access legislation could exacerbate the loss of privacy. Though the grounds that privacy rights are important civil rights could be considered sufficient to establish the loss of privacy as a putative social problem, the grounds that lawful access legislation lacked proper oversight measure adds another dimension to the problem. The putative increase of requests for information, the widespread use of personal information on a global scale, and the inability to confirm how the data was used would make it difficult to verify that Canadians' privacy rights were respected and that their personal data was handled in accordance with legal standards, leaving Canadians unaware of any infringement upon their privacy rights. As a consequence of this, citizens would be rendered unable to evaluate the consequences of lawful access and hold the state accountable for the loss of privacy rights, further undermining the democratic relationship between citizens and the state.

Privacy and Political Partisanship

As discussed previously, claims-makers who belonged to political parties that opposed the government in the House of Commons – such as the Bloc Québécois, the Liberal Party, and the New Democratic Party – recognized the risk that lawful access would result in a loss of privacy rights. However, the political opposition's resistance to lawful access was much more nuanced and was not solely grounded in the content of the legislation and its implications. Rather than reject lawful access legislation outright, the political opposition provided general support based on the grounds that potential privacy problems could be settled during committee discussions. To quote Liberal MP Mark Holland and NDP MP Jim Maloway during the discussions of Bill C-47:

Mr. Speaker, a number of stakeholders have raised the concern of accessing Internet service provider records without the use of a warrant. They have acknowledged that there is a significant oversight mechanism after the fact but the problem is with what we do beforehand. One of the things we will need to look at in committee is how we provide timely access to police to ensure they are able to go after the individuals who are committing serious crimes and have the ability to chase after those who have a huge technological advance on them. (Holland, 2009b, p. 6250)

It will also provide law enforcement agencies with access under an accelerated administrative process without a warrant or court order. That is a big issue with the NDP and it concerns us a lot. On that basis, we want to make certain that in committee we can make some changes to the bill that will further protect the privacy of citizens in this country. (Maloway, 2009, p. 6329)

Both clearly mobilized the grounds that, while there were potential privacy problems with the legislation, committee discussions would be sufficient to resolve these problems. This part of the claims-making process demonstrates Bigo and Tsoukala's (2008) arguments that political debates about (in)security are "the result of structural competition between actors with different forms of capital and legitimacy over contradictory definitions of security and different interests" (p. 4-5). The above quotes represent two such different interests.⁴³ First, the Liberal Party and the NDP both expressed support for privacy rights; the evidence of this is in the fact that Mark Holland was concerned that "a number of stakeholders have raised the concern of accessing Internet

⁴³ Political partisanship presents a third interest. As opposition parties, the Liberal Party and the New Democratic Party had a political interest in undermining the then-Conservative government. The way the opposition parties co-opted the claims-making process of lawful access legislation to make political attacks against the Conservative government is examined later in this chapter.

service provider records without the use of a warrant” and that Jim Maloway stated the NDP wanted to “make some changes to the bill that [would] further protect the privacy of citizens in this country.” As claims-makers, they both clearly established that they considered Canadians’ privacy rights to be important.

The second interest is security. Though critical of Bill C-47’s effect on privacy rights, Mark Holland provided assurances that the Liberal Party wanted to “provide timely access to police to ensure they are able to go after the individuals who are committing serious crimes and have the ability to chase after those who have a huge technological advance on them,” and while Jim Maloway’s words did not discuss security issues or investigative powers, MP Don Davies, another representative of the NDP, made a statement similar to Mark Holland’s while discussing the potential implications of Bill C-46 and Bill C-47:

Now, the concept of having Bill C-46 and Bill C-47 together is something that we, as parliamentarians, have to be very cognizant of because, as all members of this House know, bills do not operate in isolation. Laws do not operate in isolation. One law may have impacts on another. In this respect, New Democrats are going to be working very hard to achieve a balance between preserving Canadians' privacy and ensuring that our police and our judiciary have the tools they need to effectively fight crimes committed over the Internet or in the digital world. Case closed. (Davies, 2009, p. 6211)

Like Mark Holland and Jim Maloway, Don Davies agreed that privacy rights were important, stating that “preserving Canadians’ privacy” was one of the NDP’s goals, but also that privacy rights needed to be balanced with “ensuring that our police and judiciary [had] the tools” required to investigate internet crimes. Thus, while the potential loss of privacy rights was part of the rhetoric, claims-makers who represented the opposition parties did not believe it was such

a severe risk that lawful access legislation as a whole needed to be rejected. By integrating the motif of the balance between security and privacy into the rhetoric, these claims-makers established the grounds that security and privacy were both necessary goals that needed to be addressed simultaneously; supporting the legislation without changes would undermine privacy, while opposing the legislation outright would undermine security. By mobilizing the motif of balance, claims-makers were delegated the political debate to committee discussions, essentially taking for granted that the committees could change the legislation in a way that would remove any potential problems, and used the committee discussions to avoid taking a firm position against – and arguably for, as the decision to wait for committee discussions could be considered vague either way – lawful access legislation. Like they agreed that lawful access legislation could result in a loss of privacy, claims-makers agreed that a rhetorical debate on the issue should be entrusted to the relevant committee, and they agreed that giving law enforcement prompt access to any data they might obtain through lawful access was an important priority. Based on the data, it is reasonable to say that privacy, as a rhetorical motif, was politically useful because it acknowledged the importance of an important political right, but MPs were unwilling to allow the state and its law enforcement agencies to be constrained by privacy rights. Their rhetoric expressed sympathy and support for privacy without taking a strict commitment in favour of privacy rights, and they were similarly supportive of expanding law enforcement powers through lawful access.

In fact, members of the Liberal Party claimed responsibility for the development of lawful access legislation by citing bills they had proposed in the past:⁴⁴

⁴⁴ The legislation in question is Bill C-74 (2005).

It was, in fact, a Liberal government that introduced this bill in 2005 and it was the Conservative Party that took us into the polls at that time and killed this legislation. Then the member for Notre-Dame-de-Grâce—Lachine introduced a private member's bill in the next session of Parliament that sat on the order paper. It was the same bill before us today. Who killed that? The Conservative Party. (Holland, 2009b, p. 6227)

Second, if the Conservatives finally understood that technology had changed and that the bill we tabled four years ago needed to be implemented, why on earth would they have introduced the bill at the end of the last session in the last week before the summer, not giving us the opportunity until today to actually vote on it? Why were they dragging their feet? Why were they delaying bringing in this legislation for which we have been calling for so long? (Holland, 2009a, p. 6180)

This statement establishes the grounds that the Liberal Party had long supported lawful access and that its legislation had been killed by the Conservative Party, explicitly accusing the Conservatives of delaying the legislation by causing an election that “killed” the Liberals’ 2005 attempt to pass lawful access legislation, “killing” a private members’ bill that contained lawful access provisions, and introducing Bill C-46 at an inconvenient time, “dragging their feet” instead of introducing the legislation sooner so that the House of Commons could debate and vote on it, essentially accusing the Conservative government of neglecting a security risk instead of treating it like an important priority. Mark Holland’s rhetoric also provides further evidence that, during the time period of Bill C-46 and Bill C-47, facilitating lawful access and supporting law enforcement was a higher priority for the Liberal Party than preserving privacy rights. The putative social problem identified in the quote above is not that the Conservative legislation threatened to erode privacy rights, but that the Conservative had blocked past attempts to

“modernize” the legislation. While Mark Holland did criticize the legislation’s surveillance measures, this critique framed the problem as a transient – the committees would discuss and then resolve it somehow. In comparison, the time the Conservative government “wasted” before introducing its own legislation is framed as an irresolvable problem. The logical solution would be to simply introduce the legislation, which the Conservatives. However, instead of supporting the legislation after the delays, Mark Holland (2009a) used the to question the Conservative government’s competence: “[W]hy on earth would they have introduced the bill at the end of the last session in the last week before the summer, not giving us the opportunity until today to actually vote on it? Why were they dragging their feet? Why were they delaying bringing in this legislation for which we have been calling for so long?” (p. 6180). The solution became accusations that implied the Conservatives’ efforts were disingenuous and that they did not take the need for lawful access seriously enough. This suggests the Liberal Party, as represented by Mark Holland, considered security and lawful access to be more important – and perhaps more politically useful – than the privacy rights they entrusted to committee discussions.

Furthermore, the Liberal Party’s position towards Bill C-46 and Bill C-47 exposes claims-makers’ need to be seen as respecting democratic rights while also having an interest in being able to use surveillance to exercise the state’s power. Accusing the Conservative Party of neglecting lawful access legislation while touting their own past legislation allowed the Liberals to portray themselves as more competent or trustworthy on security issue, and their comments on changing the legislation in committee to address privacy risks also shows a willingness to protect Canadians’ personal privacy. This rhetorical approach demonstrates the tension embedded in the balance between security and privacy: while political claims-makers involved in surveillance policy have an interest in being seen as protecting democratic privacy rights, they also have an

interest in implementing surveillance measures they can potentially influence or control depending on electoral results, allowing them to exercise surveillance power.

The grounds that the Liberal Party had long supported lawful access legislation later became a liability for the party's claims-makers.

When discussing Bill C-30, Liberal MP Francis Scarpaleggia asked questions about the possible loss of privacy, strongly implying that lawful access legislation would be used to spy on Canadians without reason or to suppress political activities:

Mr. Speaker, the government is preparing to read Canadians' emails and track their movements through cellphone signals, in both cases, without a warrant. How can we trust the Conservatives with such sweeping powers when they use Facebook to keep law-abiding Canadians out of a public meeting? Is this 2012 or 1984? How can we trust them not to use private information to intimidate law-abiding Canadians gathering, for example, to protest a pipeline or to protest pension cuts? (Scarpaleggia, 2012, p. 5196)

The Conservative government responded to these accusations by citing the Liberal Party's historical support for lawful access legislation. Vic Toews, who was the Minister of Public Safety at the time and who also sponsored Bill C-30, issued the following response to Francis Scarpaleggia's questions:

Mr. Speaker, I thank the member for the opportunity to tell him that every province unanimously supported moving forward with the legislation, legislation that was introduced first under the Liberal government, by his party.

As technology evolves many criminal activities, such as the distribution of child pornography, become much easier. We are proposing to bring measures, to bring our laws into the 21st century and provide police with lawful tools that they need.

He can either stand with us, or with the child pornographers. (Toews, 2012b, p. 5196)

By making this statement, Toews subverted the Liberal Party's past support for lawful access, which was used to accuse the Conservatives of not taking lawful access reform seriously enough, and used it as grounds to implicitly accuse the Liberal Party of hypocrisy due to the shift in their stance and to explicitly accuse the Liberals of supporting pedophiles because of their concerns about the potential loss of privacy rights, and while the Liberals had previously sought to implement their own lawful access legislation to "modernize" surveillance measure for a government under their political control, they chose to respond to Bill C-30 by taking a stricter stance against surveillance than they had in the past.

While the Liberal Party's shift could be interpreted as rhetorical inconsistency or a change in policy, there is one point of consistency that was present throughout the debates about lawful access legislation: the motif of political partisanship.⁴⁵ Political parties, as claims-makers, sought to establish grounds that they could be trusted to implement "proper" lawful access legislation that would protect both Canadians' security and their privacy rights, while their political opposition could not.

⁴⁵ Though the specific example used here focuses on the Liberal Party, political partisanship was used as a motif by all political parties, as discussed in the following analysis. Likewise, Vic Toews comments that Francis Scarpaleggia, and by extension, the Liberal Party as a whole, could support the Conservative Party's legislation or support pedophiles are partisan in nature.

When the loss of privacy was raised as a social problem, political claims-makers often associated it with the Conservative Party as a way of delegitimizing the government formed from their political opposition. For example, Bloc Québécois MP Nicolas Dufour specifically linked the potential for privacy violations or obtrusive surveillance in Bill C-46 to the Conservative government:

Quand je parlais de problématique, il ne faut pas non plus tomber dans l'autre extrême. C'est là que j'ai une crainte face aux conservateurs, et peut-être plus face à l'aile réformiste et allianciste des conservateurs. Avec ce projet de loi, on peut facilement dépasser les limites. (Dufour, 2009, p. 6221)

Though Dufour acknowledged that the bill itself could go beyond the acceptable limits of surveillance, his statement focused on the fact that Bill C-46 was Conservative legislation, associating the problem with political partisanship rather than privacy as a civil right. This contrasts with other claims that situated the putative loss of privacy inside the legislation. Returning to the grounds that committee discussion could resolve potential privacy problems, Mark Holland mentioned that stakeholders had “raised the concern of accessing Internet service provider records without the use of a warrant” (Holland, 2009b, p. 6250) and Jim Maloway said that the NDP wanted to “make certain that in committee we can make some changes to the bill that will further protect the privacy of citizens in this country” (Maloway, 2009, p. 6329). The claims-makers’ grounds that committee discussions could address the loss of privacy are based on the premise that the problem, if it existed, was present in the legislation, as studying and amending legislation is the task of parliamentary committees. Moreover, Mark Holland, as discussed previously, stated that the Conservative Party had not acted quickly enough and had presented Bill C-46 later than they should have.

Instead of situating the loss of privacy inside Bill C-46, Nicolas Dufour attributed it specifically to the Conservative government, and rhetorically constructed the loss of privacy as a social problem that could not be solved by committee discussions, as the committees had no authority to replace the government.

The way the rhetorical motif of partisanship directs the loss of privacy away from the legislation and towards a specific political party has significant implications that can be examined through the lens of condition-categories, classifications that define what a social problem is really about (Ibarra and Kitsuse, 1993). Claims based on the motif of the balance between security and privacy define the social problem as about security risks or infringement of privacy rights, but the motif of partisanship makes the social problem about a political party, thereby rhetorically constructing a social reality wherein the loss of privacy is not a problem because lawful access infringes upon privacy rights, but because lawful access is putatively controlled by the Conservative party. Meanwhile, the other political parties are rhetorically insulated from accusations that their surveillance measures would infringe upon privacy rights simply because they do not include themselves in the condition-category defined by their rhetoric; by making the loss of privacy about the Conservative government, the opposition parties set the grounds that the loss of privacy cannot be about them.⁴⁶

⁴⁶ It should also be noted that, as the governing party, the Conservatives exerted more direct control over the state's surveillance apparatus. Grounds that the opposition parties would abuse lawful access would not have been credible, as the opposition parties had no such power. However, Vic Toews' statement that Francis Scarpaleggia could stand with the government or the child pornographers utilizes the motif of partisanship to implicitly associate child pornography with the Liberal Party and the other opposition parties, creating a condition-category that makes child pornography, cybercrime, crime, and other putative security problems about the opposition parties, thereby establishing the Conservative government as more effective on the issues of crime and safety. Though the grounds are different, the rhetorical motif and its objectives are fundamentally similar.

One Liberal MP, Judy Foote, went so far as to associate the surveillance measures of lawful access legislation with then-Prime Minister Stephen Harper's "people," further emphasizing the partisan nature of the grounds:

In its current form, Bill C-30 forces Internet service providers to track, save and hand over Canadians' personal subscriber information, including their email and IP addresses, upon request without a warrant. This means that the Prime Minister's people would now have the legal right to monitor the emails of Canadians and track their movements online without any kind of judicial discretion. (Foote, 2012, p. 5563)

Instead of critically re-examining the legislation and its privacy implications, the opposition parties seemed more interested in constructing grounds that specifically associated the loss of privacy with the governing Conservative Party. These grounds created an implicit distinction between the condition-categories of "bad" lawful access proposed by the Conservatives and "good" lawful access that would ostensibly come from the opposition. Thus, while this rhetoric presented opposition to lawful access legislation, it did not actually oppose the content of the legislation, nor was it based solely on the potential loss of privacy rights. The way claims-makers associated the Conservative Party with surveillance and the loss of privacy shows how partisan affiliation can become part of the rhetorical process to oppose other political parties without necessarily opposing the fundamental basis of their policies. The rhetorical motif of partisanship was very clearly used to define the loss of privacy as an inherently *Conservative* problem and create an implicit distinction between the Conservative legislation and the other party's policies – even when those policies directly supported lawful access. Thus, the rhetoric excluded the opposition parties from the aspects of lawful access they considered most problematic, and in

instances such as Foote's above comments, went so far as to insulate the Canadian State from the problem by attributing it specifically to the Conservative Party.

The rhetorical motif of partisanship also has important implication for social problem theory, as it clearly illustrates how motifs situate social problems and direct the rhetoric. Because the motif of the balance is based on security and privacy, it lends itself to a rhetoric that focuses on policy issues and discussion of fundamental democratic rights. The rhetorical motif of partisanship does not. Instead, it lends itself to rhetoric that constructs social problems based on nominal party affiliation, with policy taking on a secondary role. As Bigo and Tsoukala (2008) note, actors who are involved in surveillance – such as the claims-makers who represent political parties – have different interests, and the motif of partisanship exposes how those interests can displace important discussions of how surveillance should be implemented and how privacy rights should be protected.

The rhetorical motif of partisanship continued into the discussions of Bill C-13. When Bill C-13 was presented, Liberal MP Sean Casey compared it to Bill C-30 and associating the legislation with Vic Toews in particular rather than focusing solely on the content of the legislation:

When Vic Toews introduced his odious and unconstitutional esnooping bill last year, a bill that would have allowed widespread government invasion into the privacy of Canadians without a warrant, he did so, to his credit, up front. He did not try to hide it—well, not too much. Faced with fierce opposition to such a massive assault on the privacy of Canadians, he famously said of the member for Lac-Saint-Louis, “He can either stand with us or with the child pornographers.” (Casey, 2013, p. 1445)

Mr. Speaker, here we are with the very minister who stood in this House one year ago and said that the provisions of Bill C-30 were not coming back and that they had listened to Canadians.

There are 47 clauses in the bill, and 37 of them are from Bill C-30, so the minister who stands up in self-righteous indignation about the Liberals and what is in the code, on 37 instances, has broken his word to the Canadian people. (Casey, 2013, p. 1447)

Sean Casey acknowledged the risk to privacy rights by describing Bill C-30 as an “esnooping bill” that “would have allowed widespread government invasion into the privacy of Canadians.” However, the rhetorical focus of his statements was not on the legislation, but on Vic Toews. Bill C-30 was referred to as “his [Toews’]” bill specifically, and the similarities between Bill C-30 and Bill C-13, after the Conservatives had announced, according to Casey, that they would not pursue Bill C-30 and that its clauses would not be brought back, were used to show grounds that Toews and the Conservatives had lied and should not be trusted – and implicitly cast doubt on the grounds used by the Conservatives to build their own rhetoric about the legislation.

The Conservative Party was even brought into grounds that did focus more on the substantive content of the legislation, such as NDP MP Jasbir Sandhu’s comments on Bill C-30:

There are six pieces of information that can be obtained, among them a person's name, address, email address and Internet protocol address. The Conservatives are saying that they have reduced the list from 11 to 6 identifiers. The previous bill contained 11 identifiers. What the Conservatives will not say is that there is a back door, which means that they would be able to add additional identifiers without any scrutiny by Parliament. There are regulations in the bill.

This morning the Minister of Public Safety said that the government would not be adding additional identifiers. Are the Conservatives prepared to take that proposed section out of the bill? (Sandhu, 2012, p. 5568)

From the standpoint of privacy rights, reducing the identifiers available through lawful access from eleven to six should be considered a positive change, but the grounds that the number of identifiers could be increased maintained the possibility that privacy rights could be further eroded, and the way Jasbir Sandhu pressed the Conservatives on the issue by asking them to remove their “back door” implied that their stated intent to limit the number of accessible identifiers was disingenuous, again linking privacy invasion and loss of rights to a party instead of a law.

Thus, the opposition parties positioned themselves as both pro-security and pro-privacy by largely agreeing that security risks needed to be addressed through lawful access legislation while acknowledging the possible infringement of privacy rights, even if it was only to refer the matter to committee for further discussion. At the same time, the rhetorical motif of partisanship allowed them to attribute the most problematic elements of lawful access – the potential infringement of privacy rights – specifically to the governing Conservative Party, which insulated them from accusations that they would also utilize lawful access to “spy” on Canadians. Though there is no data available to confirm the opposition parties’ intention, the social problems constructed by their claims-making activities – security risks, the loss of privacy, and the governing Conservative party – are explicitly identified in their rhetoric.

Domain and Orientation

Using the grounds discussed above, privacy advocates expressed domain statements – definition statements used to “examine phenomena and determine which do, and which do not,

fall within the defined category's domain" (Best, 1987, p. 104) – that positioned the loss of privacy rights as a matter of fundamental democratic rights. The grounds that privacy was an inherently important civil right and that lawful access legislation lacked sufficient oversight measures spoke to the democratic relationship between the state and its citizens. Similarly, the grounds that the Conservative Party, as the governing party, could not be trusted to implement lawful access legislation and would use its surveillance powers to spy on Canadians express doubts about the democratic relationship between citizens and the Conservative-governed state. These grounds worked together to construct lawful access legislation as a social problem because it would allow an unaccountable state to infringe its citizens' personal privacy.

Extending from this domain, the orientation of the grounds – aspects of the definition statements that "guide the way we interpret the problem, suggesting appropriate avenues for response" (Best, 1987, p. 105) – pointed to political solutions. Though claims-makers discussed grounds that could arguably indicate a legal orientation, such as police involvement or oversight measures, these same grounds also have significant political implications because they describe the relationship between the state and its citizens according to claims-makers. Framed in this context, facilitating the state's ability to request citizens' personal information without implementing sufficient oversight or transparency creates an unequal political relationship between the state, which is not held accountable for its surveillance practices, and its citizens, who are subjected to state surveillance. The political implications of the loss of privacy as a social problem are most obvious in the motif of partisanship, which the opposition parties used to claim that the Conservative government specifically could not be trusted with lawful access powers. The rhetoric expressed by privacy advocates and members of the opposition parties defined the loss of privacy not simply as a matter of legal procedure, but as a political problem.

Reviewing the Grounds of the Loss of Privacy

In the context of lawful access legislation, the grounds used to construct the rhetoric of the putative loss of privacy were based on the inherent importance of privacy rights to democratic governance, the anti-democratic nature of widespread surveillance and information requests without oversight measures to keep it in check, and specifically partisan accusations that the Conservative Party could not be trusted with such surveillance measures, despite other political parties sharing common grounds with the Conservatives on security issues, investigative powers, and new technologies at various points in the claims-making process. The inherent importance afforded to privacy rights established the foundation of the loss of privacy as a social problem: any infringement on privacy rights is cause for concern because it represents the loss of both an individual legal right and a collective constraint on state power that protects the space for democratic governance. Meanwhile, the expansion of lawful access and the lack of oversight established the putative reality of this problem. According to claims-makers, lawful access legislation could facilitate information requests in ways that did constitute a loss of privacy rights, and the lack of necessary oversight made it difficult, if not impossible, to measure the extent of the problem and ensure that privacy rights would be respected.

Yet, privacy rights were not the only concern, nor were they treated independently of other factors. The data shows that political partisanship was an important motif to claims-makers who were formally affiliated with the opposition parties of the House of Commons. These claims-makers demonstrated a consistent ability and willingness to adapt their policy position towards lawful access legislation, either accusing the Conservative Party of not updating lawful access legislation quickly enough or accusing them of using lawful access to erode privacy rights. This part of the rhetoric is evidence, Bigo and Tsoukala's (2008) argument that

surveillance policies could be influenced by a variety of competing interests, that claims-makers' stance on surveillance and privacy was at least partially influenced by broader politics and by their willingness or ability to leverage those issues to improve their own position or undermine their competition. Because social problems are rhetorically constructed by the claims-makers' assessment of putative social conditions, the content of lawful access legislation was not the only factor considered by claims-makers when they decided their rhetorical position and defined lawful access as problematic. They situated their claims-making activities in the context of their broader political needs and constructed their rhetoric accordingly.

Warrants

Because the rhetorical warrants used to construct a claim create a logical link between the claim's factual grounds and its conclusion (see Best, 1987; Toulmin, Rieke and Janik, 1984), they are necessary to explain why claims-makers consider lawful access legislation a risk to privacy rights. Grounds such as the importance of privacy as a democratic right, the frequent nature of information requests, or the lack of oversight for surveillance measures define social conditions, but they do not explain *why* those conditions should be considered problematic.⁴⁷ Warrants such as the balance between security and privacy and the importance of democratic rights that explain why the putative social conditions constitute a loss of privacy and why this loss of privacy should be considered a social problem according to claims-makers.

⁴⁷ Because rhetorical warrants can be oblique or implicit (Best, 1987), the distinction between grounds and warrants is not always clear. The statement that privacy is an inherently important civil right could be considered a statement of fact about the nature of privacy rights as well as an implied warrant that the loss of privacy rights, a critical democratic right, constitutes a social problem. Due to the overlap, such motifs are examined as both grounds and warrants, focusing on different aspects and implications depending on the different places they occupy within the rhetoric. As grounds, the importance of privacy rights primarily establishes that any infringement on privacy rights qualifies as a form harm, while as a warrant, it establishes that these harms are problematic.

The Balance of Security and Privacy

The need to balance between security and civil rights is a common theme in the fields of security, surveillance, and privacy (see Baker, 2003; Bannister, 2005; Neocleous, 2007), and this is reflected in the claims-making activities contained within my data; the need to maintain a proper balance between security and privacy was an important rhetorical warrant to claim lawful access legislation would result, with multiple claims-makers constructing their claims based on the warrant that maintaining this balance was necessary in order to preserve Canadians' democratic rights. As Liberal MP Judy Foote directly said, "[i]f Canada is to remain a truly democratic society, it must strike the correct balance between security and civil liberties and individual rights and freedoms" (Foote, 2012, p. 5563). This particular framing of the balance explicitly positions both security and civil liberties as necessary elements of Canada as a "truly democratic society," which implicitly supports claims-making activities that favour security over civil liberties by treating security and civil rights as equally important rights. That said, Judy Foote's words directly acknowledge that privacy was a matter of civil rights necessary to democracy, providing further evidence of a rhetorical warrant that privacy, warrants, oversight, accountability, and transparency are democratic rights that must be acted upon.

This warrant explains some of the grounds used by claims-makers who belonged to the Bloc Québécois, the Liberal Party, and the New Democratic Party. On the basis that the balance between security and civil rights – in this case, privacy rights – is a moral warrant that justifies policy claims, it would be logical for them not to reject security concerns outright. This would explain why claims-makers emphasized the role of parliamentary committees, suggested they could address any potential loss of privacy caused by lawful access legislation. Rhetorical grounds that favoured privacy rights too heavily according to their assessment would have

violated the balance as a warrant, while grounds that acknowledged the potential loss of privacy without labeling it as inevitable created an oppositional rhetoric that was still compatible with the balance of security and privacy as a warrant.

From this perspective, the grounds that the Conservative Party's policy mismanaged lawful access – either by not introducing the legislation quickly enough or by including surveillance measures that eroded privacy rights – take on a different meaning. They are not a purely partisan attacks, but rather attempts to construct the Conservative government as the problem by accusing it of failing to maintain the necessary balance. Grounds that the Conservatives did not introduce lawful access legislation quickly enough establish that they failed to uphold the balance's security objectives. Grounds that the Conservatives included measures in the legislation that violated privacy rights establish that they failed to protect privacy rights. The warrant also shows how, despite adopting different grounds, the claims-makers of the political opposition maintained a coherent rhetoric. Whether they accused the Conservatives of failing to protect Canadians or of spying on Canadians, their claims-making activities still utilized the balance between security and privacy as a rhetorical warrant.

Moreover, the privacy rights guaranteed by the Canadian Charter of Rights and Freedoms raise the notion that privacy *is* security due to the characters of the judicial process. As Françoise Boivin, an MP of the NDP, noted:

Some of you, such as you, Ms. Reda, have seen the justice system. It's not the fastest thing in the world and it's very highly emotional for victims who go in front of it. So imagine if you pass one, two, three years in front of the system just to see the warrant being struck down and all the proof that was with it struck down. That's what we're trying to avoid. So it's not protecting the cyberbullies. It's making sure that in our framework we

have a Charter of Rights, we have some laws that have to be applied, we have some jurisprudence, and everything fits together. (Boivin, 2014, p. 14)

This quote expresses a warrant that is also based on the balance between security and privacy, but that filters privacy rights through a purely pragmatic lens rather than calling upon their inherent significance. Françoise Boivin tied privacy rights to proper legal procedures to suggest that some prosecutions could fail because important evidence was not accessed through the proper procedures and according to the proper privacy standards. This creates a warrant that the loss of privacy is a social problem because it could result in the release of criminals in the future, thereby undermining the security surveillance seeks to maintain.

On the subject of oversight, Leo Russomano, a representative of the Criminal Lawyers' Association, argued that “[t]he higher the expectation of privacy is, the higher theoretically the standard ought to be” (Russomano, 2014, para. 256), a warrant that advocates for increasing privacy standards according to privacy expectations in order to respect Canadians’ understanding of their own privacy.⁴⁸ As a rhetorical warrant, this argument is also implicitly based on the balance between security and privacy. However, it uses more specific terms that better represents the rhetorical claims of privacy advocates who opposed lawful access legislation in stricter terms. Rather than relying on a nebulous “balance,” Leo Russomano asserted that the requirements to access information should scale with the expectation of privacy, a standard that, while subjective, establishes a more concrete privacy standards that acknowledges the inherent importance of privacy rights. According this warrant, the loss of privacy is established through the grounds that lawful access legislation grants immunity to organizations that share

⁴⁸ Several information and privacy commissioners expressed a similar sentiment, writing in a newspaper article that “[n]ew surveillance powers must not come at the expense of our right to privacy” (Clayton, Denham, and Cavoukian, 2012, para. 6).

information with law enforcement without demanding a warrant and grounds that the legislation does not provide sufficient oversight to keep track of privacy violations. These grounds establish that, according to claims-makers, the putative social conditions of lawful access contribute to the loss of privacy.

Altogether, these warrants represent, in one way or another, the putative balance between security and civil privacy rights, whether due to the needs of a democratic society that demands both security and privacy, the risk that improper procedure would cause criminals to be released, or the need to scale oversight and information access requirements should scale with privacy expectations. All these warrants are based on the moral foundation that a loss of privacy occurs when privacy rights are not respected.

Democratic Civil Rights

The strictest warrant by which the loss of privacy is determined is also a prominent motif in the rhetorical ground discussed previously. To quote Marian Brown (2014) once more: “infringement of a charter protected privacy interest is a harm” (p. 9). To privacy advocates who are less concerned by security needs and who do not have a vested interest in political partisanship, the fact that infringing upon the privacy rights guaranteed by the charter constitutes a form of harm – and therefore, a rhetorical warrant that determines the loss of privacy – is self-evident.

Though the right to privacy could be considered important on its own, some claims-makers sought to support its rhetorical credibility as a warrant by linking privacy to other democratic rights, thereby situating privacy rights within the broader context of democratic politics. To do this, Steph Guthrie presented privacy as a matter of consent:

Perhaps most of Bill C-13 isn't really about cybersexual assault, but I find it interesting that it violates some of the same privacy principles, such as freely given and specific consent. Most of us do not and would not give free and specific consent for the state to access any, and potentially all, of our data by way of our Internet service providers if we had any meaningful choice in the matter. (Guthrie, 2014, p. 6)

By referencing cybersexual assault, consent, and choice as rhetorical motifs, Steph Guthrie framed privacy rights as a matter of personal autonomy and decision-making agency – two elements necessary to democratic politics, as a democracy is meant to govern with its citizens' consent. From this perspective, the harms caused by the loss of privacy rights should be evaluated similarly to the harms caused by cyberbullying and cybersexual assault, as both involve a violation of consent.

In another instance, David Fraser addressed the immunity to civil liability in the context of damages and reparations to emphasize that the sharing of personal information should be considered a form of harm:

It says that you will not be liable for handing over any data that you're not prohibited by law from handing over, and if you do so you're civilly immune. Now, only the criminal law and other regulations create prohibitions against handing over information, but you can hand over information when you're not legally prohibited and still incur civil liability. Civil liability is there for a reason. I may not be legally prohibited from accidentally 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. (Fraser, 2014, p. 3)

The warrant implied here is that citizens should be entitled to some form of compensation if they are harmed – such as when their privacy rights are infringed upon. That Bill C-13 prevents citizens from holding third parties liable when their personal information is shared undermines the very concept of legal protection; according to this rhetoric, citizens can no longer trust that the government will respect their civil rights.

The Conclusions of the Claim

As discussed previously, the grounds that privacy rights are important to democratic society, that lawful access legislation lacked oversight mechanism, and that responsible use of surveillance measures was heavily influenced by party affiliation established factual evidence that lawful access legislation would erode privacy rights, while the warrants of the balance between security and privacy and of the importance of democratic right explained that the putative loss of privacy should be considered a social problem because it risks begins it brings into question the state's relationship with its citizens, and raises the possibility that the state could intrude upon personal spaces in ways that undermine fundamental principles of democracy such as the freedom of speech. Following this rhetoric, this section examines claims-makers' conclusion that lawful access would result in a loss of privacy rights that would be problematic to Canadian society as a whole. Liberal Senator Serge Joyal outlined this issue clearly when discussing the content of Bill C-13:

The other element that concerns me is that when there is a challenge on a provision of a Charter, there are always three questions that the court will walk through. The first is: What is the purpose of the legislation? Is it a sound purpose? Second, does the measure proposed in the legislation under discussion serve the objective that the purpose is supposed to get? Third, is it the least intrusive? In my opinion, the least intrusive question

will fail because at least presently, when you get a search warrant or an authorization to tap someone's line, you have to inform the person after that you have done it in order for there to be a balance, but not with this anymore. Now you can get much more information than the wiretap and you don't even have the obligation to inform the person that you got all the information about the privacy of that person. It seems to be one of the key elements that will bring those measures to fail in the court. (Joyal, 2014, p. 241)

Citing the grounds that lawful access lacked necessary oversight and the warrant that oversight was necessary to protect privacy, Serge Joyal claimed that Bill C-13 did not respect Charter rights and that at least some of its measures would be considered too intrusive according to legal standards. Likewise, Liberal MP Wayne Easter claimed that "the courts could ultimately find that many of the provisions of Bill C-13 would be illegal" (Easter, 2014a, p. 8118). These claim-makers claimed that not only would lawful access infringe upon privacy rights, it would infringe upon privacy rights to the extent that it would not be considered legal and would therefore constitute an infringement upon citizens' democratic rights.

In addition to this, there were also more specific claims that the mass collection of information, combined with a lack of regulation and oversight, would allow police to obtain and share personal information with little to no judicial oversight, essentially operating outside the rule of law that is supposed to regulate the relationship between the state and the citizens and codify citizens' basic civil rights. As NDP MP Charmaine Borg put it:

En enlevant cette réflexion préalable à la transmission des données, essentiellement, on ouvre grand la porte au partage de renseignements personnels; on crée et encourage un système qui fonctionne complètement à l'extérieur d'une quelconque supervision judiciaire; on crée un système qui fonctionne à côté de toute supervision parlementaire; et

on crée un système qui exclut presque toutes les autorités qui devraient avoir le droit de jeter un regard à ces activités. (Borg, 2013, p. 1521)

According to this claim, the lack of oversight would compound the loss of privacy caused by lawful access and enable police to conduct illegal surveillance on a massive scale. This goes beyond concerns about excessive surveillance and privacy intrusion, and it illustrates how different privacy issues are intertwined within the broader context of governance relationships.

When asked about the immunity from civil liability, Daniel Therrien said that “this kind of activity [information requests] should take place under defined parameters, under clear legal thresholds, with transparency mechanisms, and with reporting mechanisms” (Therrien, 2014, p. 8), referencing mechanisms – legal thresholds, transparency, reporting – by allowing them to assess how lawful access was applied. Similarly, Michael Geist said that “from an individual perspective, the lack of notification in these instances [where telecommunication companies share information with the government] is enormously problematic,” (Geist, 2014a, p. 9) echoing the claim that surveillance was problematic and would lead to a loss of privacy rights if it did not occur within a regulated context.

There were also claims that the civil immunity granted by the legislation could amount to a form of coercion. As feminist advocate Steph Guthrie said to the Standing Committee on Justice and Human Rights, “it is also debatable the extent to which a person might feel compelled to provide the information to a police officer, even if technically they are volunteering to do so” (Guthrie, 2014, p. 6). Though the analysis of the grounds primarily examined the civil immunity included in Bill C-13 as the removal of a barrier that would discourage third parties from sharing information with the state, Steph Guthrie’s claim suggests that third parties would feel *obligated* to provide information on request. The provision of immunity from civil liability

goes beyond the rhetorical construction of the loss of privacy as a social problem and shows how privacy is entangled with democratic rights that are meant to protect citizens from the state's influence. The social problem presented in this rhetoric is not simply that privacy rights would be infringed upon, but that requests for information would become inherently coercive – a direct exercise of state power that would be implicitly impossible to refuse.

Speaking of Bill C-13's broader political and legal implications, Steph Guthrie also commented that "Bill C-13 enshrines the idea of transferable consent in law, immunizing anyone who shares our information and violates our privacy without adequate legal justification for doing so," (Guthrie, 2014, p. 6) essentially claiming that the legislation would remove citizens' ability to consent to searches while allowing telecommunication companies and other organizations to consent to the searches on behalf of their customers. This is yet another example of how the rhetoric not only constructed the loss of privacy as a social problem, but also extended the issue to other rights.

Chapter 5: Loss of Privacy, Part 2

As noted in earlier chapters, the need to balance security and freedom or privacy is a common motif in discussions of security, surveillance, and privacy rights, and much of the research on surveillance focuses on how policymakers' attempts to maintain this balance can undermine privacy rights. Scholars such as Baker (2003), Lyon (2003), Bannister (2005), and Mathiesen (2013) all argue that many surveillance measures are implemented in response to a security threat such as terrorism, prioritizing security over privacy rights that some consider critical to democratic society.⁴⁹ As Bannister (2005) puts it, privacy can be considered "a valuable good which can be traded voluntarily for other goods or benefits" (p. 76) such as security measures. Likewise, Pozen (2016) argues that "[p]rivacy is constantly being juxtaposed with competing goods and interests, balanced against disparate needs and demands" (p. 222). Based on this interpretation of privacy, it can be reasonably argued that, according to many scholars, the balance between security and privacy is an important concept to the field of surveillance studies, and studies often examine the issue as a trade-off between security measures justified by the risk of security threats and citizens' privacy rights, often to the advantage of expanding security measures.

On the other hand, Bigo and Tsoukala (2008) argue that political debates about (in)security are "the result of structural competition between actors with different forms of capital and legitimacy over contradictory definitions of security and different interests" (p. 4-5), an argument that provides a greater degree of nuance raising questions about how, exactly, proponents of security measures approach democratic privacy rights. Privacy is, according to Bannister (2005), a fundamental human right, and so it is reasonable to expect that an excessive

⁴⁹ These issues are discussed in chapter 3 and chapter 4.

loss of privacy rights could be problematic for elected politicians.⁵⁰ The private sector also provides evidence that public concern for privacy rights can influence policy; according to Rozenshtein (2018), consumer demand for privacy protection has discouraged technology companies from assisting government surveillance programs. This creates space for privacy-protective legislation. For example, Gao (2025) examines how European data protection authorities and other institutions such as the “the Article 29 Working Party (WP29—a transgovernmental network of DPAs), the Directorate-General for Justice and Consumers (DG Just—a rights-oriented department of the European Commission), the ECJ, and the European Court of Human Rights (ECtHR)” (p. 338) were able to leverage their resources and collaborate at the supranational level to successfully advocate for privacy laws across Europe. Accordingly, while the state does routinely curtail privacy rights to expand security measures, the loss of privacy rights is not completely unchecked.

In short, while some researchers argue that privacy rights are regularly curtailed to the benefit of security measures, others examine how privacy rights can be successfully protected. According to the evidence, the erosion of privacy rights is not inevitable, and that there is some nuance to the relationship between security and privacy. That nuance is the subject of this chapter.

The previous chapter analyzes claims that lawful access legislation was a social problem that would cause a loss of privacy rights. Privacy advocates and opponents of lawful access

⁵⁰ Calo (2016) discusses the various social conditions that elected politicians must negotiate, including their constituents’ diffused demands for privacy rights, intelligence agencies’ focused demands for surveillance, and the secrecy and lack of transparency that can make it difficult to monitor surveillance programs. Though Calo (2016) notes that the competing interests between citizens and intelligence agencies create obstacles to privacy rights and often favour surveillance over privacy, there are some instances where politicians reinforced privacy rights in specific and limited contexts, such as when the United States Congress decided to “require more process before the NSA [National Security Agency] can access these [phone data] records” (p. 31).

legislation claimed that lawful access would infringe upon privacy rights integral to democratic society, that the legislation lacked necessary oversight to prevent abuse and keep the state accountable for its surveillance measures, and that the Conservative government specifically could not be trusted to respect Canadians' privacy. This chapter examines how proponents of lawful access legislation constructed the claim that the legislation would, in fact, *protect* privacy rights.

From a rhetorical perspective, both claims are based on the rhetorical idiom of loss and agree on the common grounds that privacy is an important civil right. Per Ibarra and Kitsuse (1993), "[t]he concept of *protection* assumes a central position in [the rhetorical idiom of loss's] remedial discourse" (p. 33, emphasis in original); if the general loss of privacy was not a social problem, there would be no need to protect privacy rights. However, the sense of loss was mobilized in contradictory ways in the data. Thus, claims that lawful access legislation would devalue privacy and claims that lawful access legislation would protect privacy used the same rhetorical idiom but reached different conclusions.

In order to understand how proponents of lawful access legislation constructed the rhetorical claim that the legislation would protect privacy rights, this chapter begins by examining the grounds mobilized in their claims, including the trivialization of personal information, the putative strength of the oversight measures applied to lawful access, and the normalization of modern surveillance based on its similarities to older surveillance practices. It then discusses how proponents of lawful access integrated the motifs of obligation and of the balance between security and privacy to establish a rhetorical warrant that justified their claims about lawful access legislation. Finally, it analyzes the conclusion that lawful access would protect privacy rights, utilizing the concept of counterterrheterics to better understand how

proponents of lawful access legislation directly contradicted claims that the legislation would undermine privacy rights.

Grounds

This section examines the rhetorical grounds – statements made to establish the factual basis of a claim (see Toulmin, Rieke and Janik, 1984; Best, 1987) – used by claims-makers to construct lawful access legislation as a form of privacy protection. Analyzing my data, I identified three major motifs used in this specific claim. First, the information available through lawful access was trivial and giving the government access to it would not significantly compromise Canadians' privacy. Second, the legislation contained oversight measures that reinforced privacy rights. Third, the new surveillance powers contained within the legislation were functionally identical to pre-existing surveillance methods and thus would not change citizens' daily lives. It is with these grounds that proponents of lawful access legislation established the claim that the legislation would adequately protect privacy rights, not undermine them.

The Trivialization of Personal Information and Surveillance

The trivialization of personal information is a general category of grounds used by government officials, politicians and police to support the general claim that lawful access would not violate privacy rights for the simple reason that the information police were seeking should not be considered private in the first place. As police representative Carson Pardy put it, the information law enforcement agencies would be able to gather under Bill C-13 was comparable to "using a licence plate number called in as a tip to the police about a dangerous or impaired driver" (Pardy, 2014, p. 4). According to these grounds, the personal information available through lawful access was comparable to publicly-available information – a licence plate number

that is openly displayed and that can be read by anyone who sees it.⁵¹ Such information could not, according to Carson Pardy, be considered private and should, in fact, be communicated to police in order to assist with their investigations.

Similarly, Public Safety Canada published a website of “myths and facts” about Bill C-30 that portrayed basic subscriber information as unimportant:

Giving authorities access to basic subscriber information does not give them either the technical ability or the legal authority to monitor personal communications and activities. Basic subscriber information would be limited to a customer's name, address, telephone number, email address, Internet Protocol (IP) address, and the name of the telecommunications service provider. It absolutely does not include the content of emails, phones calls or online activities. (Public Safety Canada, n.d., p. 1)

The above quote shows how the Conservative government defined privacy and personal information at the time of Bill C-30 by making a distinction between “personal communications and activities” (which would be private) and “basic subscriber information” that included “a customer’s name, address, telephone number, email address, Internet Protocol (IP) address, and the name of the telecommunications service provider” (which would not be private). In the context of Bigo and Tsoukala’s (2008) argument that political actors often hold different definitions of security, this quote also shows how they can hold different definitions of privacy; while privacy advocates mobilized grounds that any infringement of privacy rights constituted a

⁵¹ These specific grounds referenced by Carson Pardy also raise the rhetorical idiom of endangerment, as discussed in Chapter 3. As discussed in Chapter 3, Chapter 4, and in this chapter, the balance between security and privacy is a prevalent rhetorical warrant in the context of lawful access legislation. Rhetorically increasing security threats while minimizing the privacy implications of personal information allowed proponents of lawful access to establish the grounds that the need for security was significantly greater than the privacy risks of lawful access. Thus, proponents could claim that the legislation would respect the balance between security and privacy.

clear harm, the government's position was that disclosing information about the content of activities or communications would be a violation of privacy, but disclosing trivial information about who was communicating and how should not be considered personal or private.

In addition to trivializing the information made available to police through lawful access, claimsmakers who supported lawful access legislation also sought to undermine the general concept of privacy on the grounds that personal information was becoming increasingly public and thus should not be considered secret, as described by Conservative Senator Linda Frum during the debates about Bill C-13:

On the concept of reasonable expectation of privacy, isn't it fair to say that there is much less privacy than most of us Internet users appreciate or recognize as is? So when you're trying to find that level of reasonable expectation, you have to remove the ignorance out of it for people who use Facebook or Google; it is not actually private. Facebook is monitoring every single transmission you make. They hang on to it, own it, monitor it, target you and market to you and sell it. They don't respect your privacy at all. I'm very anti-Facebook. (Frum, 2014a, para. 260)

When there is a reasonable suspicion, then law enforcement can have access to it as well, but my privacy is already being violated as is. No? (Frum, 2014b, para. 170)

These grounds show how proponents of lawful access defined privacy. Rather than focusing on the content of the information, on the details it might reveal, or on the ownership of the information, the grounds focus on how the information is distributed, rhetorically constructing information as private only if it belongs to a single party or possibly if it is communicated directly between parties. According to these claims-makers, communicating information through

a third party intermediary to a broad audience should set the expectation that the information is no longer private. On that basis, then, any information that is shared between an individual and a third party intermediary, such as basic subscriber information that represents the subscriber's personal information but that must also be shared with the organization that provides the subscription service, is no longer private and should be accessible to law enforcement agencies and other government authorities.

The trivialization of personal information and its implications for privacy were accompanied by grounds that sought to trivialize and normalize the surveillance practice of lawful access as well, such as when Conservative Minister Peter MacKay said that that Bill C-13's lawful access measures were "in keeping with existing police and court practices around warrants and around seizures, while at the same time responding to the very real technical aspect of how data is preserved, relayed, and treated in the Internet and the electronic world" (MacKay, 2014b, p. 7).⁵² By normalizing lawful access in this manner, the rhetorical grounds constructed its surveillance measures as a trivial issue – a practice identical to other surveillance practices that were already a familiar part of Canadian society and that should not be considered a loss of privacy rights.

⁵² Similarly, police representative Timothy M. Smith wrote in a newspaper article that:

The inspector clause is very similar to clauses that have been written into numerous legislation: the Bankruptcy and Insolvency Act, Customs Act, Department of Transportation Act, and even the Feeds Act contain the same type of clause contained in Bill C-30. It is there to ensure compliance and in no way means that authorities may "take any information Ottawa wants" (Smith, 2012, para. 3).

As rhetorical grounds, this statement normalized Bill C-30 and lawful access legislation in general by equating it to five other laws which were, according to Smith, both similar to Bill C-30 and implicitly non-problematic. Thus, Bill C-30 should not be considered a "new" form of surveillance, nor should it be considered abnormal or excessive surveillance beyond the commonplace surveillance Canadians were already subject to.

All these grounds – that subscriber information was not important enough to be private, that lawful access was equivalent to other surveillance practices, that some personal information was already widespread through third parties and could no longer be considered private – rhetorically constructed subscriber information as information that the state could reasonably access without infringing upon privacy rights because citizens should not expect it to be private. Additionally, the normalization of lawful access, which was compared to other surveillance measures, defined lawful access as a common element of everyday life that Canadians were used to, setting up the implication that the legislation would neither change Canadians' experience of privacy nor allow the state to obtain information it did not already have access to. As such, the motif of trivialization and normalization presented putative grounds that lawful access legislation would protect privacy because it would not be used to obtain information that should reasonably be considered private.

Oversight Measures

While privacy advocates claimed that lawful access legislation did not contain sufficient oversight to ensure it would not infringe Canadians' privacy,⁵³ proponents of the legislation claimed the opposite. Their rhetoric described the oversight provided by lawful access legislation as sufficient, rhetorically constructing the legislation as a means to protect privacy rather than subvert it. Unlike the academic interpretation of privacy as something to be sacrificed for the sake of security (see Bannister, 2005), my data demonstrate that proponents of lawful access expressed great concern about Canadians' privacy rights and insisted that they would be respected *through* the legislation itself. As early as Bill C-46, Conservative MP Brent Rathgeber stated that "any disclosure of information under all of these legislative proposals would be

⁵³ See Chapter 4.

pursuant to a judicial authorization" (Rathgeber, 2009, p. 6208), establishing that lawful access would be subject to judicial oversight and that the state would not be able to request information arbitrarily, thereby ensuring that lawful access would not be used to unlawfully spy on Canadians or invade their privacy. Later, Minister of Public Safety Vic Toews defended Bill C-30 by explaining that it would only be used by a limited number of officials, preventing potential abuses and providing necessary oversight for accountability:

Bill C-30 would put in place a system of checks and balances that simply does not exist today, including the fact that officials would have to be designated to make subscriber information requests. Only a limited number of officials would be allowed to be designated to request basic subscriber information, either five individuals or 5% of an agency's workforce, whichever is greater. It would be set out in the law that all requests for basic subscriber information would have to be made in the performance of a duty or a function of the agency in which the designated official is employed. (Toews, 2012a, p. 5549)

When Bill C-13 was put forward, Conservative MP Peter MacKay touted that "[t]he bill requires judicial oversight" (MacKay, 2014a, p. 8107), once again emphasizing the grounds that lawful access legislation included sufficient oversight measures. The government's position was that legal precautions and restrictions had been put in place to ensure that there would be no violation of privacy rights. As such, lawful access would not, according to these claimsmakers, allow the government to spy on Canadians arbitrarily, nor would it infringe upon privacy rights.

The grounds that lawful access contained sufficient limitations was not only expressed by politicians and government employees, but by legal experts and members of civil society who were asked to testify about the legislation. For example, Monique St. Germain, then general

counsel of the Canadian Centre for Child Protection, endorsed Bill C-13 on the grounds that it would protect privacy rights:

Thirdly, concerns have been raised that Bill C-13 unduly interferes with the rights of Canadians under section 8 of the charter. The bill has two important safeguards: the requirement to apply for a warrant, and judicial discretion to issue or not issue the warrant. Police have a duty to make full, frank, and fair disclosure of all material facts to the issuing judge when they apply for a warrant. (St. Germain, 2014, p. 3)

According to Monique St. Germain, Bill C-13 required a warrant,⁵⁴ which would ensure that police would need to provide a “full, frank, and fair disclosure” before requesting information and that a judge would verify the request and concern that it met the required legal standards. Rhetorically, these grounds downplay the increase in police powers and construct lawful access legislation not as a loss of privacy, but as the very law that would protect Canadians’ privacy and prevent infringement upon their democratic rights.

Police representatives also utilized these grounds in their rhetoric, drawing upon their position and professional experience to explain how lawful access measures would protect Canadians' privacy; when testifying before the Senate committee on Legal and Constitutional Affairs about Bill C-13, Ontario Provincial Police Detective Inspector Scott Naylor said that “[a]ccess to this information would be strictly controlled and limited to law enforcement officials, who would be fully trained in these procedures and subject to auditing and report oversight” (Naylor, 2014, para. 62).⁵⁵ As claims-makers, police representatives insisted that the

⁵⁴ As discussed in Chapter 4, privacy advocates claimed that lawful access legislation would not require a warrant.

⁵⁵ In a newspaper article written in support of Bill C-30, police representative Jim Chu stated that “[o]nce subscriber information has been obtained, it is only with a warrant based on reasonable grounds to believe a crime has occurred that police can then use the information to investigate alleged web-based criminal activities of individuals” (Chu, 2012b, para. 4).

legislation's regulations included warrant requirements and strict oversight that would protect privacy rights by confirming the legitimacy of any information requests and limiting the surveillance powers to a few law enforcement officers so that lawful access requests would not be in widespread use.

The Canadian Association of Chiefs of Police (CACP) also denied that lawful access would allow police unrestricted access to personal data and infringe upon privacy rights:

This is absolutely not true. This legislation is not designed to do away with the need for a warrant for information currently obtained by way of warrant. This legislation is designed to bring the Criminal Code into this century and this decade and provide for the ability to preserve data that might not otherwise be retained, to allow for law enforcement agencies to apply for the warrants to obtain the information. Crimes involving the use of services and sites available on the internet are on the increase – from child exploitation to identity theft – and law enforcement agencies require the ability to obtain the data required to determine whether the person suspected has committed a crime. This information could only be obtained with the issuance of a warrant by a judge. (Canadian Association of Chiefs of Police, n.d., p. 9)

Here as well, the rhetorical grounds sought to establish lawful access legislation as a form of privacy protection through warrants and judicial oversight, ensuring privacy rights would be respected. Notably, the CACP's rhetoric did not suggest that privacy rights should be curtailed in order to facilitate surveillance. Rather, their statement mobilized the motifs of security and privacy as coexisting concepts, setting the grounds that lawful access would support police investigations without undermining privacy, which allowed proponents of lawful access legislation to claim that it would only be used in a manner consistent with privacy rights.

The way the motif of oversight was used to construct the grounds that lawful access legislation contained sufficient oversight can be understood through the motif of security. According to Côté (2016), studies of security should approach the audience of the security discourse as active actors who possess agency, not merely subjects of a security regime that seeks to strip away their privacy rights. This explains why proponents of lawful access legislation were so concerned about protecting privacy; a rhetoric based on the grounds that privacy rights had to cut back for the sake of security would likely be rejected by Canadians. Indeed, the public's perception of police legitimacy is positively related to legal boundaries (Huq, Jackson and Trinkner, 2017) and people are more likely to believe police are legitimate when their actions are perceived as just, fair, and neutral (Mazerolle, Antrobus, Bennett, and Tyler, 2013). Likewise, Tyler and Huo (2002) argue that the most effective way for police to secure the public's compliance is to demonstrate that "they are using fair procedures in exercising their authority, and that their motives are trustworthy" (p. 7). Thus, it was necessary – or at the very least, convenient – for proponents of lawful access to establish grounds that legitimized lawful access by emphasizing that it would protect privacy rights and that it would only be used in a fair and just manner. Citizens' perception of fair, procedure-based law enforcement increases police legitimacy and encourages the public to cooperate with law enforcement officials (Jackson et al., 2012), and the perception of legitimacy increases the public's "willingness to empower the police" (Moule, Parry, Burruss, and Fox, 2019, p. 96). Grounds that emphasized the oversight measures contained within lawful access legislation allowed claims-makers to address the protection of privacy and related civil rights, thereby making the claim that the legislation would protect the democratic relationship between the state and its citizens. Through the motif of oversight, the rhetorical motif of privacy protection combines security and privacy rather than

positioning them as opposing forces. Lawful access was presented as the means through which warrant and oversight requirements would be codified into law to secure privacy rights, guaranteeing that surveillance would only be used through legitimate means and for legitimate purposes, and assuring Canadians that their privacy rights would not be infringed upon.

Normalization of New Surveillance by the Old

In addition to claiming that the information available through lawful access was trivial and shouldn't be considered private and that lawful access legislation contained enough oversight to protect Canadians' privacy and prevent abuses, proponents of lawful access also normalized lawful access by comparing it to older, pre-existing technologies. The security-based claim was that lawful access had to be modernized to adapt to new technologies,⁵⁶ but proponents of lawful access mobilized seemingly paradoxical grounds to build the claim that lawful access legislation would not grant police new powers; during debates about Bill C-47, Conservative MP Shelly Glover said that:

I want to be clear, however, that the proposals we are putting forward are not new or even revolutionary. In modernizing Canada's lawful access laws, we are not providing new powers or expanding on existing interception authorities that have been in place since 1974, nor are we compromising individuals' personal information, or putting an undue burden on business. We are simply bringing our country's legislation out of the cold war era and into the 21st century. (Glover, 2009, p. 6225)

This particular quote demonstrates the rhetorical paradox expressed by the grounds. The explicit purpose of the legislation was to modernize lawful access. Yet, Shelly Glover's statement

⁵⁶ See Chapter 3.

equated lawful access legislation with laws that had been in place since 1974 and compared them to surveillance practices that were used during the Cold War, promising to bring them “into the 21st century” and update them without creating any truly new powers adapted to modern technologies. The grounds established here described lawful access legislation as new within the context of 21st century technology, yet described them as old and familiar in the context of privacy rights. In doing so they established putative social conditions that lawful access legislation would be adapted to modern technologies but would neither change the state’s access to citizens’ personal information nor risk infringing upon their privacy rights.

Similar grounds were expressed about the other bills. On the matter of Bill C-30, Conservative MP Dave MacKenzie said that:

If I were to conclude my remarks at this point, I might leave the impression that Bill C-30 is more or less privacy neutral, that it just maintains the existing safeguards and replicates those safeguards for new investigative powers. However, such an approach without more would fail to take stock of the profound effect that technological advances over the past few decades have had on privacy. (MacKenzie, 2012, p. 5587)

Describing Bill C-30 as “more or less privacy neutral” provided grounds to claim that it would maintain privacy standards and would not implement any changes that would infringe upon citizens’ rights. Additionally, Dave MacKenzie’s statements further illustrate how claims-makers situationally constructed lawful access legislation as old or modern. The grounds that the legislation “just maintains the existing safeguards and replicates those safeguards for new investigative power” create a clear indication that lawful access should be considered old and established in the context of privacy rights, but new in the context of police investigations. This

rhetorical construction addressed the putative need to modernize surveillance powers and the need to maintain the pre-existing balance between state power and citizens' privacy.

Similarly, Conservative MP Peter MacKay, who was the Minister of Justice at the time, insisted that Bill C-13 both would and would not give police new powers:

Mr. Speaker, that is in fact the very crux of the issue, striking that balance between protection of online activity while at the same time giving police modern powers with judicial oversight. There were certainly criticisms and legitimate concerns raised in the past and with respect to the bill about unlawful access online to information. The bill requires judicial oversight. The bill does not create new powers for police that go beyond the Criminal Code. It does not allow for any new online investigation without judicial oversight. (MacKay, 2014a, p. 8107)

Again, the rhetoric presented the seemingly paradoxical grounds that the legislation would give police modern powers implicitly adapted to new telecommunication technologies while promising that these powers would neither “create new powers for police that go beyond the Criminal Code” nor “allow for any new online investigation without judicial oversight.” The framing of this particular quote is conditional, as it allows for new police powers that are *within* the Criminal Code. What this means in practice is more immediately evident, but it does imply that any new powers provided by lawful access legislation would merely replicate pre-existing surveillance or investigative powers and apply them to modern technologies, thereby modernizing surveillance powers without needing to create any new powers. Once again, this rhetoric allowed claims-makers to establish the grounds that lawful access legislation would be simultaneously new for investigative and security purposes, yet old and familiar for the purposes of privacy protection.

The rhetorical motif of new and old surveillance powers was also used to support lawful access legislation's oversight measures. In particular, the sections that would, according to some privacy advocates,⁵⁷ allow peace officers and state representatives to request information from third parties without a warrant, were compared to other, pre-existing laws by proponents of lawful access. Conservative MP Larry Maguire described it as a clarification based on pre-existing laws:

This is a very important point, because there have been concerns expressed that section 487.0195 is somehow creating a new power requiring companies to provide access to information. It is not a new power, it is merely a re-enactment of an existing “for greater certainty” clause, nor does it contain any requirement to co-operate with a request.
(Maguire, 2014, p. 4623)

For reference, section 487.0195 of Bill C-13 states the following:

487.0195 (1) For greater certainty, no preservation demand, preservation order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing.

(2) A person who preserves data or provides a document in those circumstances does not incur any criminal or civil liability for doing so. (Bill C-13, 2014, p. 24)

According to Larry Maguire, that particular section was not a new law, but a “re-enactment” of some other existing clause. According to these grounds, it was always possible for peace officers

⁵⁷ See Chapter 4.

or public officers to request information voluntarily, so the inclusion of the specific clause in Bill C-13 was merely a matter of clarification to reaffirm existing surveillance practices. Therefore, it would not constitute a new form of surveillance power and should rather serve as another example of how lawful access legislation protected privacy rights by preserving pre-existing privacy standards.

By using the rhetorical motif of new yet old surveillance measures, claims-makers who supported lawful access constructed rhetorical grounds that emphasized the legislation's benefits while denying its privacy risks. The way claims-makers equated the investigative and surveillance powers of lawful access legislation to other, pre-existing powers created grounds to claim that the legislation would protect privacy rights because the state's access to citizens' personal information would remain the same. This rhetorical approach is similar to the process of normalization often discussed in the fields of security and surveillance. According to Agamben (2004) and Neocleous (2006), states regularly respond to putative emergencies and security risks by adopting exceptional laws and measures that are retained and extended until they become the new norm. Over time, exceptional emergency measures become familiar and normalized. The motif that lawful access measures are simultaneously old and new provides an example of how this takes place in a rhetorical context by pre-emptively normalizing any aspect of lawful access that could be considered "new." The grounds equated lawful access to existing privacy safeguards, to surveillance measures that had been in place since 1974, and to powers were already within the purview of the Criminal Code. Claims-makers used surveillance powers and privacy expectations that had already been normalized to create grounds for the claim that lawful access legislation would not infringe upon privacy rights and would, in fact, protect privacy by operating within existing legal standards.

Domain and Orientation

The grounds discussed above were not used to claim the existence of a social problem caused by lawful access legislation. On the contrary, they provided factual evidence that the legislation would, in fact, protect privacy rights. However, the concept of protection is, as noted by Ibarra and Kitsuse (1993), closely associated with the rhetorical idiom of loss, and the grounds that lawful access legislation would protect privacy rights would only be rhetorically relevant if the loss of privacy rights was both a possibility and a social problem. The domain statements expressed by the grounds – statements that “examine phenomena and determine which do, and which do not, fall within the defined category's domain” (Best, 1987, p. 104) – are relevant not because of what they include in the social problem of the loss of privacy, but because of what they *exclude*. The trivialization of personal information rhetorically excluded the information available through lawful access from the private sphere, justifying the government’s ability to request it. Additionally, the grounds that the legislation included sufficient oversight measures and would replicate pre-existing surveillance practices without creating new forms of surveillance excluded lawful access from the domain of intrusive surveillance. In this manner, the rhetorical grounds excluded lawful access legislation from the broader concept of the loss of privacy as a social problem.

By excluding lawful access legislation from the domain of problematic and intrusive surveillance, proponents of the legislation positioned it as the solution to the loss of privacy, claiming that it would, in effect, Canadians’ privacy rights, thereby orienting the loss of privacy towards a legal remedy. According to these claims-makers, lawful access legislation would limit the state’s ability to obtain citizens’ private information, lawful access legislation would implement mechanisms that would hold the state accountable for its surveillance practices, and

lawful access legislation would preserve surveillance standards that Canadians were already familiar with. Unlike privacy advocates who based their claims on political issues such as the importance of civil rights or political partisanship,⁵⁸ supporters of the legislation claimed that its provisions, such as the oversight measure and the (putative) fact that the legislation did not allow lawful access to target truly private information, would be sufficient to prevent government abuses and protect citizens' privacy rights.

Warrants of Obligation and Balance

To support their claims that lawful access legislation would protect privacy, the legislation's proponents utilized a rhetorical warrant that integrated the motif of government obligation and the motif of the balance between security and privacy. During discussions about Bill C-13, Conservative Senator Thomas Johnson McInnis made an explicit link between privacy protection and government obligation, stating that "[r]esponsible governments have to weigh the balance" (McInnis, 2014, para. 342). The statement that the governments "have" to weigh emphasized that action was a necessary obligation, and maintaining the balance was an objective for the government to achieve. Lawful access legislation, as an extension of the Canadian government, also had to balance security and privacy. Thus, the legislation had to protect privacy – a devaluation of privacy rights would mean the government had failed to meet its obligations.

Linking the grounds to the warrant, Conservative MP Peter McKay raised the need to balance security and privacy while speaking about Bill C-13:

Mr. Speaker, that is in fact the very crux of the issue, striking that balance between protection of online activity while at the same time giving police modern powers with

⁵⁸ See Chapter 4.

judicial oversight. There were certainly criticisms and legitimate concerns raised in the past and with respect to the bill about unlawful access online to information. The bill requires judicial oversight. The bill does not create new powers for police that go beyond the Criminal Code. It does not allow for any new online investigation without judicial oversight. (MacKay, 2014, p. 8107)

According to this statement, the grounds that Bill C-13 required judicial oversight and did not grant police any new powers proved that the legislation maintained a proper balance between security and privacy, thereby protecting privacy rights. Moreover, Peter MacKay raised the “criticisms and legitimate concerns” associated with “unlawful access to online information,” explicit evidence that the rhetorical claim that lawful access legislation would protect privacy rights was based on the acknowledgement that the loss of privacy would constitute a social problem. Without these “legitimate concerns,” there would be no rhetorical need to claim lawful access legislation would protect privacy.

The rhetorical effectiveness of this warrant of obligation and balance can be seen in the fact that representatives of the opposition parties agreed with it. During debates about Bill C-13, NDP MP Andrew Cash argued that “[w]e need to be clear that the foundation of a liberal democracy is the protection of civil liberties” (Cash, 2013, p. 1527), leverage citizens’ democratic rights, including privacy rights, to claim that the government should not intrude upon Canadians’ personal information. Likewise, Liberal MP Dominic Leblanc asked the government to assure Canadians “that warrantless searches and the appropriate balance between the privacy rights of Canadians is respected while at the same time allowing the full prosecution of these horrible offences [such as child pornography] to take place” (Leblanc, 2014, p. 8107), referencing the balance between security and privacy to construct the rhetorical claim, as

Conservative representatives did, that the Canadian government was obligated to maintain said balance when implementing lawful access legislation. Though the representatives of the NDP and the Liberals may have *attempted* to question the government's ability to properly balance investigative powers and privacy rights,⁵⁹ their rhetoric was also based on the motifs of balance and obligation and their claims used the same warrant. Thus, they could not oppose the fundamental premise of the claims-makers who supported lawful access legislation. Rather, their rhetoric provides a practical example of Bigo and Tsoukala's (2008) argument that security measures are influenced by different actors who possess different interests and different definitions of security. The claims made by privacy advocates and proponents of lawful access shared grounds and warrants based on very similar rhetorical motifs: privacy and personal information, oversight and accountability, and the balance between security measures and privacy rights. The rhetorical conflict between the two groups of claims-makers was not located in the premise of their claims, but in the putative social conditions constructed by their respective interpretation of the grounds – what Bigo and Tsoukala (2008) would refer to as “contradictory definitions of security” (p. 5).

Drawing upon the grounds that lawful access legislation would only be able to access unimportant and impersonal information, that its surveillance measures were unobtrusive, and that it contained sufficient oversight measures to prevent privacy infringements, the warrant of obligation and balance and supported the claim that lawful access legislation would protect privacy rights. Through the motif of the balance between security and privacy, the trivialization of personal information and surveillance measures rhetorically lowered the threshold for privacy infringement, which created an allowance for more surveillance practices. The grounds gave

⁵⁹ See Chapter 4.

privacy less “weight”, thereby reducing the significance of the harms caused by privacy violations. Thus, increasing surveillance measures to access this trivial, non-private information would respect the rhetorical warrant that the government had an obligation to maintain the balance between security measures and privacy rights. In this manner, the rhetorical warrant framed lawful access legislation as a means to protect said balance and preserve privacy standards.

Likewise, the motif of oversight found in the grounds reduced the putative risk of privacy violations; they would be prevented or detected by the oversight measures, protecting the privacy of Canadians and preserving the balance. Adding to this, the motif that lawful access legislation paradoxically modernized and replicated existing surveillance practices addressed the balance directly, claiming that citizens’ experience of security and privacy would not be changed by lawful access legislation and reaffirming that their privacy rights would not be negatively affected. The motif of government obligation reinforced the claim, both justifying the legislation as a matter of necessity and implying that, because the government had a responsibility to maintain the balance between security and privacy rights, its legislation inherently preserved the balance. In this matter, the warrant of balance and obligation constructed the claim that lawful access legislation protected privacy rights.

Conclusions of the Claim

Proponents of lawful access legislation claimed that the trivial nature of the personal information covered under the legislation, the oversight measures contained in the bills, and the legislation’s ability to retain existing privacy protections while modernizing investigative powers would, under the warrant of the government’s obligation to maintain the balance between security and privacy, protect Canadians’ privacy rights rather than undermine them. Based on

these grounds and warrants, claims-makers supported lawful access legislation drew the conclusion that lawful access legislation contained the necessary measures to protect privacy rights and associated democratic rights. As Conservative MP Peter MacKay said:

Nothing in Bill C-13 is intended to create any new powers to obtain information without a warrant, as has been suggested by some members of the NDP. Simply put, the bill puts forward privacy safeguards, which are built into the legislation and built into the investigative powers of the bill. It is tailored to meet those expectations around privacy, but at the same time allow the police to do this critically important work of protecting the public from online criminality. (MacKay, 2014, p. 8109)

Though this specific statement focuses on the normalization of lawful access based on pre-existing surveillance practices – specifically, by denying that the legislation would create any new powers – the conclusion can be applied to the general claim: based on the grounds that lawful access legislation did not target truly private personal information, that it contained sufficient oversight measures, and that it respected well-established surveillance methods and privacy standards, as well as the warrant that the government had an obligation to balance security needs and democratic privacy rights, lawful access legislation would effectively protect privacy rights.

The claim that lawful access would protect privacy rights can be examined through the lens of counter-rhetorics, “discursive strategies for countering characterizations made by claimants” (Ibarra and Kitsuse, 1993, p. 30). Since claims that lawful access legislation would cause a loss of privacy rights and claims that it would protect privacy rights used very similar rhetorical idioms and motifs, the claim of privacy protection can be considered a sympathetic counter-rhetoric, a strategy “which accept[s], in part or whole, the problematic status of the

condition-category, but which in effect block[s] the request for remedial activities” (Ibarra and Kitsuse, 1993, p. 38). Proponents of lawful access and privacy advocates both agreed that the loss of privacy rights would constitute a social problem. The difference was in the remedial measures: privacy advocates claimed that the following the legislative process through committee discussions and amendments would rectify the privacy risks contained in the legislation while proponents of lawful access claimed that the legislation would prevent the loss of privacy once it was implemented and did not require any modifications.

The specific counterrhetorical style used is more difficult to identify. According to Ibarra and Kitsuse (1993), the naturalizing counterrhetoric insists that a social problem is inevitable, the counterrhetoric of the costs involved argues that the addressing the problem is prohibitively expensive compared to simply enduring it, and the counterrhetoric of declaring impotence states that the resources or methods required to address the problem are unavailable. These strategies do not apply here, as proponents of lawful access legislation claimed that it would prevent the loss of privacy rights. Thus, the loss of privacy was not inevitable, the costs of protecting privacy were not considered too high, and the required resources were available.

The remaining strategies are the counterrhetoric of perspectivizing, in which “[t]he claim is characterized as an opinion” (Ibarra and Kitsuse, 1993, p. 40) and the counterrhetoric of tactical criticism, in which “[t]actical critics accept the characterization of the condition-category being proffered, but demur in the means claimants employ” (Ibarra and Kitsuse, 1993, p. 40). The data suggest that both were used to construct different aspects of the claim that lawful access legislation would protect privacy rights.

First, the counterrhetoric of perspectivizing can be seen in the grounds. As discussed in Chapter 4, privacy advocates established that lawful access legislation would allow the state to

request private information and lacked the oversight necessary to guarantee it would respect privacy rights. Conversely, proponents of the legislation stated, as discussed in this chapter, that lawful access would not be used to request truly private information and that the oversight measures it contained would ensure respect of privacy rights. Both groups mobilized grounds that were related to the rhetorical idiom of the loss of privacy, but they disagreed on whether or not these grounds described a putative social problem. Thus, whether or not lawful access would devalue privacy rights was a matter of opinion.

The counterrhetoric of tactical criticism is raised in Chapter 3, which examines the rhetorical idiom of endangerment from new technologies. To address the privacy risks of lawful access legislation, members of the opposition suggested that the Bill C-13 be split so that the measures aimed at combatting (cyber)crime and cyberbullying could proceed while the surveillance measures could be discussed further. The Conservative government refused, claiming that all measures were necessary and that they had to be combined. The claim that lawful access legislation would protect privacy rights provides a greater understanding of the government's claim that the legislation could not be split. According to members of the opposition parties, the correct tactic would have been to separate the legislation and discuss its privacy implications further. According to the government, the correct tactic was to proceed with the legislation as whole. This shows a fundamental disagreement about which means to use in order to protect Canadians' privacy.

However, this alone does not explain why proponents of lawful legislation were able to pass Bill C-13. A possible answer to this question can be found in the four stage natural history model proposed by Spector and Kitsuse (1973), particularly the first three stages: claims made about problematic putative social conditions by a group, the recognition of these claims by an

official agency capable of taking charge of the social problem, and the reaction to the official agency's handling of the social problem. The rhetorical development of lawful access did not follow this model exactly, as the original claims that new technologies endangered Canadian society and that only lawful access legislation could solve the problem were made by the official agency, combining the first two stages. However, the third stage can be seen in the claims that lawful access should have been split and that its surveillance measures would cause a loss of privacy rights.

As both the original claims-maker and the official agency charged with handling the problem, the Canadian government⁶⁰ held a privileged rhetorical position. The official agency's intervention "may lend prestige to the original protest group, but at the same time may begin to overshadow and thus reduce the significance of its activities" (Spector and Kitsuse, 1973, p. 153) or "take over the issue, making it their own, and neutralize or eliminate the original protest group" (Spector and Kitsuse, 1973, p. 153), but such a rhetorical conflict could not take place in the context of lawful access legislation because the original group of claims-makers and the official agency were the same. Though there was some resistance to lawful access legislation, as seen in the claims that it would devalue privacy rights or that the legislation should be split, that Bill C-13 became law shows that, ultimately, the resistance's claims were unconvincing. As noted by, Bigo and Tsoukala (2008), actors⁶¹ involved in security possess "different forms of capital and legitimacy" (p. 4-5). It is therefore likely that the disagreements between proponents of lawful access and privacy advocates were ultimately resolved in favour of supporting the

⁶⁰ Though this research focuses predominantly on Conservative legislation, the Liberal Party had proposed similar legislation using a similar rhetoric, as discussed in Chapter 3.

⁶¹ Or claims-makers, in the context of social problem theory.

legislation because that was the government's rhetorical position, and the government held more formal political capital and legitimacy than other claims-makers.

Additionally, the legislation's opponents agreed that new technologies were a danger to society⁶² and both sides of the debate discussed the privacy implications of lawful access using the same rhetorical idioms and motifs. The rhetorical conflict was defined by common grounds, common warrants, and common motifs, and while there were disagreements about the interpretation of the grounds and the best methods to use to protect Canadians from cybercrime, cyberbullying, and privacy invasions, these disagreements were seemingly not enough to construct a firm rhetorical opposition to lawful access legislation.

⁶² See Chapter 3.

Chapter 6: Discussion

The focus of this research is on how the legislation came into law, and the data show that the details of the legislation held little interest for claims-makers. Certainly, the claims-makers knew what the legislation was about in general, which is why they discussed issues such as surveillance, cybercrime, privacy rights, and democratic rights. However, the implications of the legislation were defined not by empirical evidence, but by subjective assessments of how lawful access legislation would affect putative social conditions. The most important finding of this research on the development of lawful access legislation in 21st century Canada is, perhaps, how little the content of the legislation mattered.⁶³

Elected officials, lawyers, police representatives, privacy advocates, and other claims-makers who, due to their education, professional experience, or position in society, could reasonably be considered knowledgeable on the topics related to lawful access constructed very different versions of it. Lawful access would infringe upon privacy rights. Lawful access would protect privacy rights. Lawful access would require a warrant. Lawful access would not require a warrant. Lawful access would modernize obsolete investigative powers. Lawful access would replicate long-standing investigative powers. Lawful access would change everything. Lawful access would change nothing. Claims-makers rhetorically constructed different bills according to their political goals, their subjective interpretations of when security, surveillance, and privacy should be considered social problems, and the putative social conditions they used to support their claims.

⁶³ Though the clauses and wording of Bill C-13 undoubtedly affected the judiciary and the legal landscape of Canadian surveillance once it received Royal Assent and came into effect, the law's consequences are beyond the scope of this research.

The many different definitions of lawful access, security, and privacy did not exist in an “objective” sense. Contradictory as they were, they could not co-exist in an objective sense. Instead, they were constructed by claims-making activities (see Spector and Kitsuse, 2017) using rhetorical idioms and motifs (see Ibarra and Kitsuse, 1993) to represent putative social conditions and present lawful access, security, cybercrime, cyberbullying, privacy rights, and democratic rights as social problems. As such, the development of Canadian lawful access legislation provides clear evidence to support the theoretical and methodological importance of social problem theory as explained by Kitsuse and Spector (1973), Spector and Kitsuse (2017), and Ibarra and Kitsuse (2003).

The data also supports Bigo and Tsoukala’s (2008) argument that political discussions are influenced by various actors – claims-makers, in the context of social problem theory – who advocate for different definitions of security, with the putative social conditions described by – and constructed by – the rhetoric representing the claims-makers’ common definitions of security, cybercrime, and cyberbullying, as well as their differing definitions of privacy, infringement upon privacy rights, and oversight.

Though the development of Canadian lawful access is obviously a specifically Canadian issue, interpreting it through the lens of social problem theory can also provide a greater understanding of how security, surveillance, and privacy policies are developed through debates between political claims-makers. As Lyon (2003) and Mathiesen (2013) note, the 9/11 terrorist attacks merely accelerated the long-standing desire to expand state surveillance and other security measures and, if that trend continues into the future, the insights gained from understanding the rhetorical construction lawful access legislation will remain politically, practically, and theoretically relevant to the field of surveillance and privacy studies. For

example, in 2026, the Liberal government of Canada introduced new lawful access legislation entitled *Bill C-22: An Act Respecting Lawful Access* (Bill C-22, 2026) to, once again, expand state surveillance powers. Accordingly, though this study focuses on past legislation, it is likely that its analysis of the rhetoric of endangerment and privacy loss will remain relevant for the foreseeable future.

This chapter synthesizes this research project and identifies key findings that require the full context of the analysis. It starts by examining how state claims-makers constructed security and security threats in order to justify the expansion of surveillance, and how they integrated specific incidents into their claims' grounds. Next, it outlines how claims-makers defined privacy in the context of lawful access legislation before moving on to different ways privacy could be conceptualized in order to develop claims beyond the motif of the balance between security and privacy. Finally, it critically discusses the four stage natural history model of social problems proposed by Kitsuse and Spector (1973) and reflects upon the methodological considerations of social problem theory.

Constructing (In)Security

The development of Canadian lawful access legislation demonstrates how states construct (in)security as a new and emerging social problem in order to position surveillance as the solution to this problem. Through their claims-making activities, members of the government, police representatives, and other proponents of lawful access legislation rhetorically constructed the claim that new technologies substantially increased criminal threats to Canadian society and created new threats such as cyberbullying. Building on this, they claimed that the only way to protect Canadians was to grant the state greater access to telecommunication technologies, expanding surveillance to better police digital spaces.

From 2009 to 2013, the motif of crime was a constant presence in the rhetoric of lawful access. Proponents of lawful access consistently used cybercrime and cyberbullying to construct technology-based crimes as a social problem through the rhetorical idiom of endangerment, claiming that the threat could only be prevented by lawful access legislation. However, the grounds claims-makers used changed significantly over the years. Prior to Bill C-30's introduction in 2012, claims-makers discussed these criminal grounds in relatively vague terms, describing cybercrime, fraud, cyberbullying, and computer-assisted crimes as threats to Canadians without attributing the threat to a specific source.⁶⁴ When Bill C-30 was being debated, then-Minister of Public Safety implicitly attributed the problem of computer-assisted crimes to the government's opposition when he said Liberal MP Francis Scarpaleggia could "either stand with us [the Conservative government], or with the child pornographers." (Toews, 2012b, p. 5196). Prior to this, members of the opposition supported lawful access legislation, agreeing with claims that new technologies presented a criminal threat to Canadian society, and while they expressed concerns about the legislation's privacy implications, they also claimed that these concerns could be addressed during committee discussions – thereby aligning themselves as the solution to the problem by offering both security measures and privacy rights.

Vic Toews' comments changed the rhetoric by shifting the social problem from new technologies to the Liberal Party and others who opposed the legislation. Following this, the opposition parties' rhetoric changed and began to focus more on the potential loss of privacy rights as a social problem. Additionally, they began to essentially accuse Vic Toews – and the

⁶⁴ It is important to note that while Bill C-46 and Bill C-47 were debated in the House of Commons, they were never brought to committee for further study. Bill C-50, Bill C-51, and Bill C-52 were introduced, but not debated. The lack of attribution in the rhetoric could be due to the limited discussion, and it is possible that the social problems could have been attributed to more specific causes if more debates and committee meetings had taken place. The available data, however, points to generic causes that were not defined in detailed and specific terms until Bill C-13.

federal government of the day – of wanting to spy on Canadians. Though previous claims that new technologies were a danger to society because they enabled crimes such as child pornography were met with agreement, claims that the opposition parties' reluctance to support Bill C-30 were equivalent to enabling child pornography were met with rejection. The data show that attributing the social problem to the political opposition did not garner support for it.

The rhetoric noticeably changed with Bill C-13 in 2013, when the social problem was no longer murky and poorly defined, but was suddenly recast in the context of specific incidents of specific harm. That legislation followed the deaths of Rehtaeh Parsons, Amanda Todd, and Todd Loik due to computer-assisted crimes such as cyberbullying, harassment, and distribution of child pornography. While Bill C-13 was being studied, Carol Todd, the mother of Amanda Todd, and Glenford Canning, the stepfather of Rehtaeh Parsons, both testified about the crimes their children had suffered. As part of the claims-making activities, these deaths and testimonies constructed specific, clearly-identified victims and created a concrete sense of dissatisfaction and danger. During the discussions of previous bills, the dangers of computer-assisted crimes were abstract concepts. During Bill C-13, they had a face.

This shift in the rhetoric has important theoretical implications. First, it illustrates a key point of social problem theory: social problems are based on subjective assessments of putative social conditions (Kitsuse and Spector, 1973), not on objective social conditions. The rhetorical motifs used to establish the grounds that new technologies were a danger to society – new crimes, old crimes, and cyberbullying – remained fundamentally the same from Bill C-46 and Bill C-47 to Bill C-13, even though the “objective” evidence was much less specific. In 2009, the endangerment of society from new technologies was a social problem according to proponents of lawful access legislation. The 2013 inclusion of Rehtaeh Parsons, Amanda Todd, and Todd Loik

in the rhetorical grounds improved the persuasiveness of the claim not because they increased its factual credibility, but because it added specificity to the nature of new technologies as a social problem. According to Spector and Kitsuse (1973), vagueness makes it less likely that a claim will be recognized and makes it more difficult for claims-makers to assign responsibility for a social problem's existence, so mobilizing the grounds that there were specific, named victims of cyberbullying increased the claim's effectiveness by decreasing its vagueness.

Second, the inclusion of specific victims of cyberbullying in the grounds provides further evidence of Lyon (2003) and Mathiesen's (2013) argument that states were expanding their surveillance and security measures prior to the 9/11 terrorist attacks, and that the attacks simply accelerated the trend. Similarly, lawful access was part of an ongoing trend; the Conservative government had introduced legislation in 2009 with Bill C-46 and Bill C-47, in 2010 with Bill C-50, Bill C-51, and Bill C-52, in 2012 with Bill C-30. The introduction of Bill C-13 in 2013 was the continuation of this trend, but unlike previous attempts, it became law. Though there may have been other contributing factors outside the scope of this project, it is still noteworthy that the "successful" claims about lawful access were the ones grounded in specific cases of cybercrime and cyberbullying. This demonstrates how claims-makers used the deaths of Rehtaeh Parsons, Amanda Todd, and Todd Loik in their claims' grounds to construct a specific rhetoric of endangerment and then used that rhetoric to push forward a policy that went well beyond the specifics of cyber-bullying by claiming that the criminalization of cyberbullying behaviours and the modernization of lawful access were both necessary in order to solve the social problem.

These two points demonstrate how policy-makers use the rhetoric of security to justify the expansion of surveillance measures at the expense of privacy rights and other civil rights integral to democratic governance. The dangerous putative social conditions remain a persistent

element of the rhetoric in order to claim there is a problem that can only be solved through surveillance measures. Specific incidents catalyze the rhetoric not because they provide “objective” evidence that it is founded on factual grounds, but because they create a more specific – and more persuasive – sense of dissatisfaction. Thus, this project shows how policy-makers sustain the expansion of surveillance over time and mobilize specific events such as 9/11 or the deaths of Rehtaeh Parsons, Amanda Todd, and Todd Loik in order to accelerate their pre-existing policy plans.

Defining Privacy

Bigo and Tsoukala (2008) claim that security policies are developed by actors with different levels of capital and legitimacy and different interpretations of security. This project shows that the same conclusion applies to privacy. Privacy rights, warrants, oversight, and evidence standards for privacy requests were important motifs in the rhetoric of lawful access, but they were defined in very different ways depending on claims-makers’ interests and political relationships. The disagreements are such that in some instances, it is impossible to determine, based on the rhetorical claims, what lawful access legislation would actually do or how it would be implemented. Claims-makers agreed that lawful access legislation would allow state representatives to request information, but could not agree on whether the evidence standards required to make a request were sufficient, whether the requests required a warrant, whether the accessible information was private, or whether the requests would infringe upon privacy rights.

Within my data, the rhetorical discussion of privacy constructed condition-categories – “the ‘society’s’ classifications of its own contents” (Ibarra and Kitsuse, 1993, p. 26) used to describe and construct social reality – based on the rhetorical idiom of the loss of privacy, sharing very similar rhetorical motifs, but reaching contradictory conclusions as to whether the

social problem of the loss of privacy applied to lawful access legislation. This alone significantly impacted the expectations of the legislation. For example, proponents of lawful access claimed that the legislation would protect privacy rights. From this perspective, the legislation contained sufficient oversight measures to ensure it would not be misused and preserved existing privacy protections. Since the legislation was positioned in this way – as protecting privacy – they argued that the information law enforcement sought through lawful access could not be considered truly private, and thus could not infringe upon privacy rights, precisely because privacy was protected by the bills.

On the other hand, privacy advocates claimed that lawful access legislation would result in a loss of privacy rights. They claimed that privacy rights were a fundamental democratic right and that any degree of infringement would be a significant harm. From this perspective, the solution to the social problem endangered the core of what needed to be protected. From this perspective, the legislation did not contain sufficient oversight measures to protect Canadians' rights, and passing it would lead to a loss of democratic freedoms. On this basis, claims-makers who were part of the Liberal and NDP parties accused the Conservative government of manifesting this loss by spying on Canadians.

My project extends the current literature on the balance between security and privacy (see Baker, 2003; Bannister, 2005; Pozen, 2016) by showing on the balance is rhetorically constructed by claims-makers who hold contradictory positions and definitions. My data show that the balance was a critical motif in the rhetorical warrants used by proponents of lawful access legislation to claim that it would protect privacy and by privacy advocates to claim that the legislation would undermine privacy rights. Both groups of claims-makers used the rhetorical idiom of the loss of privacy, based their rhetorical grounds on similar motifs, and mobilized the

same rhetorical warrant to justify their conclusions about the privacy implications of lawful access. Though researchers often conclude that security is used to justify security measures that restrict personal freedoms such as privacy rights (see Baker, 2003; Bannister, 2005; Lyon, 2003; Mathiesen, 2013), the claims-making activities that sought to define privacy based on contradicting grounds showed more nuance than the simple expansion of surveillance at the cost of reduced privacy.

Proponents of lawful access did not explicitly claim that privacy rights needed to be curtailed in favour of the modernized surveillance and investigative powers included in lawful access legislation. On the contrary, they claimed that lawful access legislation would protect Canadians' privacy by implementing sufficient oversight measures and replicating privacy protection measures present in existing surveillance laws, which would not upset the balance between security needs and privacy rights at all, and would instead modernize lawful access without making any changes to privacy rights. Furthermore, they claimed that information requests would only target subscriber data and communication metadata rather than the content of communications, so they would not be able to obtain details that should be considered truly private. Through these claims, the legislation became a self-fulfilling prophecy: the legislation protects privacy so any information released under it is not private. As such, proponents of lawful access legislation did not claim that a loss of privacy was necessary and acceptable in order to prevent social problems such as cybercrime and cyberbullying. On the contrary, they claimed that their proposed solution would maintain and protect privacy rights and the existing balance between security and privacy. In fact, it was the opposition parties who claimed that sacrificing privacy rights was necessary to protect Canadians, with Liberal MP Wayne Easter claiming that the Liberal Party recognized the privacy risks posed by Bill C-13, but that

cyberbullying was so problematic that they would support the legislation regardless.⁶⁵ The opposition parties constructed the dangers of cyberbullying and the loss of privacy as two problems with mutually exclusive solutions. Proponents of lawful access legislation, on the other hand, constructed cyberbullying, cybercrime, and new technologies as social problems, but claimed lawful access legislation would not result in a loss of privacy and should therefore not be considered a social problem.

This shows how complex the relationship between security and privacy is, especially when claims-makers rhetorically construct different definitions of what they mean. In the case of lawful access legislation, claims-makers generally agreed that new technologies, cybercrime, and cyberbullying constituted a social problem that demanded a solution. Thus, the government was able to leverage the rhetoric of endangerment to garner support for the legislation; delaying the legislation would allow the problem to persist. Conversely, privacy advocates and claims-makers who resisted or opposed the legislation could not leverage the loss of privacy to convince the government to withdraw or modify its surveillance measures because the government's claims explicitly concluded that lawful access legislation would protect privacy rights and that there was no social problem to solve. Claims-makers who claimed that cyberbullying and the loss of privacy were both social problems constructed a rhetoric that eventually forced them to prioritize one problem over the other; according to their own claims, blocking lawful access legislation would expose Canadians to the dangers of cybercrime and harassment, while implementing the legislation would undermine privacy rights. Since the government only claimed the existence of

⁶⁵ See Chapter 3.

one social problem – the endangerment of society from new technologies, cybercrime, and cyberbullying – its rhetoric did not require such a compromise.

This demonstrates the relevance of Bigo and Tsoukala's (2008) argument about the importance of capital, legitimacy, and definitions. The contradicting definitions of privacy were not simply a matter of rhetorical debate and counterclaims, nor were they a competition over the "true" definition of privacy and privacy rights. The grounds used by the government to make its claims about lawful access and privacy rights allowed it to claim that it could provide a non-problematic solution to cyberbullying and cybercrime while negating privacy advocates' claims that the legislation would devalue privacy rights. Moreover, the "successful" claims were those made by the Conservative government, which, as the government, possessed forms of capital and legitimacy that other claims-makers did not have. The government's ability to leverage its capital and legitimacy in its claims-making activities is beyond the scope of this research, but it merits further study in order to better understand how the government "imposes" its rhetorical claims. The concept of claims-making styles, for instance, examines "how various groupings of the claimant's bearing, tone, sensibility, and membership category can inform both a claim's general appearance and specific content as well as instruct auditors on how the claim should be interpreted" (Ibarra and Kitsuse, 2003, p. 40), so the membership category of claims-makers, such as their political affiliation, does affect their claims-making activities in some way.

Reconceptualizing Privacy Rights

In the context of Canadian lawful access legislation, privacy advocates were unable to escape the rhetorical framing established by proponents of lawful access. By largely accepting the claim that cybercrime, cyberbullying, cyberpredators, and other crimes associated with new technologies were a danger to Canadian society and that surveillance measures were necessary to

investigate and prevent this crime, privacy advocates conceded that some level of surveillance was acceptable, which made it difficult to construct a rhetoric that could strongly oppose lawful access legislation.

Moreover, the rhetoric of endangerment from new technologies, the rhetoric of privacy protection, and the rhetoric of privacy loss all mobilized the warrant of the balance between security and privacy to create moral justification for their claims. Thus, all claims-makers agreed, at least to some degree, that surveillance and privacy should maintain a proper balance to preserve Canadians' safety as well as their democratic rights. This meant most if not all claims-makers were predisposed to accept each other's claims on the basis of their shared warrant. Combined with the fact that most claims-makers also agreed with the claim that computer-assisted crimes posed a danger to society, this pushed the rhetoric towards supporting lawful access legislation rather than prioritizing privacy rights. This outcome is consistent with findings that the discourse often favours security over civil rights (see Baker, 2003; Bannister, 2005; Lyon, 2003; Mathiesen, 2013). However, as discussed above, the balance is not purely adversarial, and the rhetoric constructed by proponents of security and lawful access expressed clear support for privacy rights, claiming that lawful access legislation would protect Canadians' privacy as well as their personal security.

This can explain why the discourse of the balance tends to favour security over civil rights. First, civil rights advocates accept the claim that security is necessary to address some threat. Second, security advocates claim that their policies will protect both security and civil rights. As discussed previously, this creates a rhetorical contradiction for privacy advocates, who recognize the emergence of two social problems with solutions that are mutually exclusive by

their very nature, while security advocates can claim surveillance will address the security threat without devaluing privacy rights, thereby maintaining the balance between security and privacy.

In this rhetoric, security advocates elide concerns about privacy rights by claiming to protect them without critically reevaluating their importance to democratic governance: the Criminal Code must be updated to account for new forms of crime and investigative powers must be modernized, but replicating pre-existing standards and procedures is sufficient to protect Canadians' privacy. This invokes several issues that are often discussed in the field of surveillance and privacy studies.

First, it shows the asymmetrical treatment of surveillance and privacy in the context of modern technology. As Lessig (1999a) notes, modern technologies have facilitated surveillance by making it easier to record information for long-term use, but the legal standards applied to privacy rights have not been updated to account for these changes. Similarly, Steeves (2008) argues that the legal test used to establish privacy expectations does not adequately represent people's experiences with digital forms of communication. The broader literature on surveillance shows that the state does not show the same interest in modernizing privacy standards as it does in modernizing surveillance, and this project shows why: maintaining pre-existing privacy standards allows the state to claim that its surveillance policies protect privacy rights by maintaining the balance between security and privacy and by maintaining the relationship between citizens and state surveillance. Thus, citizens should expect that state surveillance will not disrupt their lives and that their personal information will remain private. Though "modernizing" surveillance while maintaining "outdated" privacy standards may increase citizens' exposure to state surveillance, the way it can rhetorically normalize new surveillance

technologies by equating them to older forms of surveillance should be considered as well, as it supports the state's claims that it can maintain the balance between security and privacy rights.

The second point concerns the oversight of surveillance measures. Though proponents of lawful access legislation claimed that it would provide enough oversight and accountability to prevent abuses, Nyst (2018) notes that “surveillance laws in fact very often fail to contain the appropriate guarantees of transparency and accountability necessary to bring surveillance into compliance with human rights standards” (p. 16), and these findings support privacy advocates' claims that lawful access legislation did *not* contain adequate oversight measures. Like the different definitions of privacy, this shows another point of disagreement between claims-makers who opposed and supported the legislation.

According to Kitsuse and Spector (1973), social problems are defined by claims-makers' subjective constructions of putative social conditions, so providing an assessment of these oversight provisions is beyond the scope of this project. However, the doubts expressed in the data by privacy advocates warrants further discussion. My research suggests that the state's unwillingness to modernize privacy rights, combined with the lack of oversight and transparency required to hold the state accountable for its surveillance practices, implies a long-term loss of privacy rights to the state. As new technologies make data easier to record in the moment and reference after the fact (Lessig, 1999a) and make it possible to aggregate data from multiple sources to obtain details on an individual's life that no single source could provide (Bailey, 2008; Haggerty and Ericson, 2000), the extension of the state's presence in new technologies will, as shown by the Snowden revelations (see Ball, 2013; Finley and Esposito, 2014; Fuchs and Trottier, 2017; Kelly, 2022), allow the state to collect information on a massive scale and

increases the risk that privacy rights will be infringed upon unless the legal and political understanding of privacy rights is modernized alongside surveillance technologies.

As seen in Chapter 4, privacy advocates claimed that privacy rights were inherently important and that any infringement upon personal privacy should be considered harmful regardless of other consequences such as criminal investigations. Similarly, Moore (2011) argues that information should be considered private not because it could be incriminating, but simply because it is private and should be respected as such. However, despite the importance of privacy rights, Hong (2017) argues that surveillance possesses the “ability and right to internally justify its own scope, validity and efficiency” (p. 188), and this project shows how policy-makers rhetorically construct security threats, normalize surveillance, and trivialize the value of personal information in order to claim surveillance can address problems such as cyberbullying while protecting privacy rights. This asymmetrical approach legitimizes the continuous expansion of state surveillance while keeping privacy constrained to a static definition that, per Steeves (2008), may not accurately represent individuals’ expectations of privacy. As the gap widens, so does the effective loss of privacy rights.

The key issues underlying this loss are the external conflict between security advocates and privacy advocates who define privacy based on different grounds and the internal conflict within privacy advocates who acknowledge security threats as a social problem while defending privacy rights. So long as the state is in a position to define privacy, it can adjust the criteria of privacy infringement to legitimize and normalize surveillance. So long as privacy advocates recognize security threats and the loss of privacy as social problems with mutually exclusive solutions, they will be forced repeat the rhetorical compromise that, as the literature argues (see Bannister, 2005; Baker, 2003; Lyon, 2003; Mathiesen, 2013), so often favours security. So long

as the rhetorical motif of the balance between security remains a fundamental rhetorical warrant in all claims made about security and privacy, it will be difficult for privacy

Breaking away from the balance between security and privacy requires a fundamental re-evaluation of what privacy is; since proponents of lawful access legislation recognized that the loss of privacy would be a social problem and yet rhetorically excluded the legislation from the condition-category of privacy loss, framing privacy as a fundamental democratic right would not be sufficient to change the rhetoric. As Hong (2017) argues, “[p]rivacy and humanism—two presently dominant frames for criticism—are necessary but insufficient for thinking about ‘another surveillance’” (p. 187) and the “debate must begin by redefining two concepts surveillance has co-opted for its own self-justification: risk and security” (p. 187). Building on this leads to a positive critique of surveillance that seeks to “tackle surveillance’s benefits head-on—sometimes by admitting them, sometimes by exposing them, sometimes by suggesting alternative means for their provision” (Hong, 2017, p. 190) rather than a strictly negative critique that focuses solely on the drawbacks and risks of surveillance. While such a critique carries the risk of repeating privacy advocates’ claims about lawful access – admitting the benefits of surveillance as a solution to cybercrime and cyberbullying, exposing how lawful access could infringe upon privacy rights by lower privacy standards or granting civil immunity to organizations that shared information with law enforcement, and proposing that the surveillance aspects of the legislation be separated and delayed for further discussion – it is, in a way, validated by the rhetoric used by proponents of lawful access legislation, who admitted the importance of privacy rights and established their own alternative definition of privacy that conveniently supported their policies. Though their rhetoric did not follow Hong’s (2017) suggested model exactly, it was based on a *positive* critique of privacy rights rather than a

negative critique that would have explicitly argued for the reduction of privacy rights. Since this rhetorical strategy was effective for proponents of lawful access, it could be useful to privacy advocates as well.

To better conceptualize security and privacy, Hong (2017) further suggests “two values that are incommensurable: the *security of way of life* on one hand, and the *security of life* itself on the other” (p. 198), defining privacy and personal safety as equally important forms of security necessary to life. Again, proponents of lawful access legislation used a similar strategy by claiming the legislation would protect Canadians from cyberbullying (i.e., the security of life) while maintaining privacy rights (i.e., the security of way of life). This distinction between different forms of security leads to a new interpretation of privacy:

Because physical survival becomes something to be defended at any cost, its defence becomes precisely the most powerful tool by which civil society and democracy can be undermined. The articulation of ‘two securities’ therefore begins by prising apart the conflation between surveillance activities and the protection of life itself. Its end is not simply to expose the socially constructed nature of security, but to arrange an explicit discussion of what kind of ‘security’ we want to construct (Hong, 2017, p. 198).

Reconstructing privacy rights as the security of a certain way of life would frame privacy as something that is equal to physical security rather than, as Bannister (2005) and Pozen (2016) find, something that policy-makers sacrifice in for the benefit of security. It would also enable privacy advocates to put privacy into direct conversation with democratic governance. While this would be unlikely to address the external conflict between proponents of security and privacy advocates (as security advocates could continue to claim that their surveillance policies protect both security of life and security of way of life), it could resolve the internal conflict of privacy

advocates by putting security of life and security of privacy on equal footing. This would make it less likely that privacy advocates would feel compelled to compromise their position on privacy in order to protect security, as the opposition parties did with Bill C-13.⁶⁶

A solution to the external struggle between security advocates and privacy advocates may be found in Petronio's (2013) report on Communication Privacy Management Theory (CPM), which focuses on privacy ownership, privacy control, and privacy turbulence, as well as eight related axioms. As discussed in Chapter 2, in privacy ownership, the first axiom "predicts that people believe they are the sole owners of their private information and they trust they have the right to protect their information or grant access" (Petronio, 2013, p. 9) and the second axiom states that "when these 'original owners' grant others access to private information, they become 'authorized co-owners' and are perceived by the 'original owner' to have fiduciary responsibilities for the information" (Petronio, 2013, p. 9). Privacy ownership and its axioms counter the claims that personal information is trivial and non-private because it is transmitted through a third party such as a website. Privacy control states that individuals retain ownership of their personal information and when that information is shared, it is shared within a context of co-ownership and comes with the responsibility to respect the private nature of the information. Communicating personal information does not imply that that information should immediately be considered public.

Under privacy control, the third axiom predicts that "because individuals believe they own rights to their private information, they also justifiably feel that they should be the ones controlling their privacy" (Petronio, 2013, p. 9), the fourth axiom predicts "that the way people control the flow of private information is through the development and use of privacy rules [...]"

⁶⁶ See Chapter 3.

derived from decision criteria such as motivations, cultural values, and situational needs” (Petronio, 2013, p. 9-10), the fifth axiom “predicts successful and continued control post-access is achieved through coordinating and negotiating privacy rules with ‘authorized co-owners’ regarding third-party access” (Petronio, 2013, p. 10), the sixth axiom “predicts co-ownership leads to jointly held and operated collective privacy boundaries where contributions of private information may be given by all members” (Petronio, 2013, p. 10), and the seventh axiom states “that collective privacy boundaries are regulated through decisions about who else may become privy, how much others inside and outside the collective boundary may know, and rights to disclose the information” (Petronio, 2013, p. 10). These axioms touch upon the fundamental concept of consent in how personal information is shared, which can be used to address the motif of oversight. They also infuse the notion of consent with agency, reinvigorating the term as part of democratic governance and not just a contractual, click-through legitimization of ongoing surveillance.

Revisiting Petronio’s work can help advance the literature because privacy control asserts that individuals believe they should decide how their personal information is used, and when the boundaries of privacy and information-sharing are expanded, it should be on the basis of established rules and agreements about who should be allowed to access and share private information and how information should be disclosed. This can create a more tangible privacy framework that is more respectful of individuals’ expectations both as consumers and as citizens. While claims-makers debated whether or not the oversight of lawful access would respect citizens’ privacy rights, oversight measures based on privacy control would respond more directly to citizens’ choices about how they want their personal information to be protected or

shared, especially with the state.⁶⁷ This concept of privacy control would allow privacy advocates to establish clear standards for the oversight of state surveillance and elicit a more specific sense of dissatisfaction when those standards are not met, which would make pro-privacy claims more convincing (Spector and Kitsuse, 1973). Faced with clear and specific demands for oversight, state representatives would need to provide equally specific grounds to support the claim that their policies would not devalue privacy rights.

Finally, privacy turbulence proposes the eight axiom, which predicts that “privacy regulation is often unpredictable and can range from disruptions in the privacy management system to complete breakdowns” (Petronio, 2013, p. 11). It acknowledges that, despite rules and agreements, the regulation of privacy and personal information can still fail. This gives privacy advocates reason to continue their claims about the loss of privacy and draw attention to privacy rights, much like how, as discussed previously in this chapter, states maintain a constant rhetoric of endangerment and insecurity in order to legitimize the continuous expansion of surveillance.

In sum, reconceptualizing privacy rights through the lens of Hong (2017) and Petronio (2013) would allow privacy advocates to move beyond the rhetorical entanglements of the motif of the balance between security and privacy so evident in my data. Defining privacy as its own form of security places physical safety and privacy on equal grounds, which would make privacy advocates less likely to concede that surveillance is necessary to protect society. Meanwhile, CPM offers concrete concepts of privacy and personal information management that can provide more specific criteria for the oversight of surveillance and create opportunities for citizens to

⁶⁷ Claims-makers who were not elected politicians did testify before parliamentary committees and make claims about the oversight of lawful access legislation, but it is impossible to tell how much influence they had over the legislation, if any.

become involved in the surveillance mechanisms that affect their democratic relationship with the state.

The Natural History Model

My research also raises questions about the state's role as a claims-maker within the four-stage natural history model proposed by Spector and Kitsuse (1973). The model states that public groups make claims about putative social conditions they consider problematic during Stage One, and that official agencies, such as the government of Canada, respond to these claims-makers during Stage Two. In the case of lawful access legislation, however, members of the government made claims about cybercrime and cyberbullying during discussions of Bill C-46 and Bill C-47 in 2009, before other claims-makers, such as information and privacy commissioners, police representatives, relatives of victims of cyberbullying, victims' advocates, and privacy advocates, made their own claims in print media or by testifying before parliamentary committees.⁶⁸ Although members of the government can and should be considered members of the public as well, the fact that they are in a position to both act as original claims-makers by defining a social problem *and* to directly decide how that problem should be addressed positions them in a unique role and possibly gives them more control and influence over the social problem's development.

From a methodological perspective, this is a significant finding because it illustrates how claims-making activities are used by governments to develop policies. Governments are not

⁶⁸ It is possible that these groups of claims-makers presented their claims to the government before Bill C-46 and Bill C-47 through means that were not apparent in my data. Additionally, the "traditional" dynamic between claims-makers can be seen in the way government representatives responded to Carol Todd's claims about privacy rights in a manner that supported lawful access legislation (see pp. 126-127), which shows that the four-stage natural history model can be applied to certain claims-making activities included in my data. This is an area that requires further research in order to better understand how communications between the state and other claims-makers took place.

strictly reactive authorities that can only respond to social problems raised by other groups. They are capable of producing their own claims and of constructing social problems in order to rhetorically support policies that advance their interests.

More importantly, the government has a great deal of influence over the development of policy. In the context of lawful access legislation, the government made claims about the endangerment of Canadian society, proposed lawful access legislation as the necessary solution to the problem, negated claims that the legislation would result in a loss of privacy, refused compromises offered by other claims-makers, and established that the legislation would, in fact, protect privacy. Best (1987) defines rhetoric as “the study of persuasion” (p. 102), but it is not clear that, within the context of lawful access, security, surveillance, and privacy, if the state can be persuaded through rhetoric alone. Though there have been successful efforts to protect privacy rights (see Gao, 2025), politicians are influenced by many interests beyond citizens’ demands (see Calo, 2016), and capital and legitimacy can both influence surveillance policies (Bigo and Tsoukala, 2008). Thus, the way governments and other official agencies position themselves as claims-makers – either by responding to the public’s claims or by producing claims that support its own policies – requires further study in order to better understand how states influence the claims-making activities used to determine surveillance and privacy policies.

Conclusion

In conclusion, this project examines how various claims-makers, such as members of the government, members of the federal opposition parties, police representatives, privacy advocates, victims' advocates, victims' families, lawyers, and others, rhetorically constructed the dangers of modern technologies and the loss of privacy rights due to government surveillance as social problems, and how these social problems were in turn used to support competing claims about lawful access legislation. On the grounds that new technologies exacerbated certain crimes, created new forms of crime, and enabled forms of cyberbullying that were particularly harmful, proponents of lawful access claimed that new legislation was required in order to protect Canadians – and claims-makers who expressed misgivings about the legislation's privacy risks also generally agreed that the legislation was required. At the same time, the legislation's proponents countered claims that it would undermine privacy rights on the grounds that it would not seek meaningful information, that it contained sufficient oversight measures, and that it would merely replicate preexisting surveillance powers rather than create new powers.

These rhetorical developments demonstrate the importance of a core motif in the field of surveillance studies: the balance between security and privacy rights. As a rhetorical motif – part of the vocabulary used in claims-making activities (Ibarra and Kitsuse, 1993) – the balance between security and privacy noticeably constrained the claims made about lawful access legislation. By serving as a common ground between claims-makers, it undermined rhetorical opposition to the legislation, as claims-makers who were concerned about its privacy implications *also* expressed concerns about the need to protect Canadians; they claimed they were compelled to support the legislation for the sake of security despite their claims that it would result in a loss of privacy rights. Rhetorically, the concept of a balance between security

and privacy led to claims that a loss of privacy was acceptable in order to protect security. The language used to make the claims did not allow for privacy and security to be socially constructed independently of each other.

The constraints imposed by rhetorical motifs can also be seen in the debates about the loss of privacy rights. Claims-makers universally agreed that privacy rights were inherently important democratic rights and that lawful access legislation should include oversight measures and restrictions to ensure it would not lead to abuses. The point of disagreement was not fundamental motifs of the rhetoric, but how they should be assessed. Privacy advocates claimed that the legislation did not do enough to respect privacy rights, while the legislation's proponents claimed that it provided sufficient oversight and protections. The disagreement stemmed from the claims-makers' contradicting evaluations of the putative social conditions – in this case, the oversight measures and privacy protections included in the legislation – and whether they should be considered problematic, not from the fundamental premise of the claims themselves. Because they were constrained by these motifs, privacy advocates could not construct alternative definitions of privacy, and proponents of lawful access legislation were able to refute their claims on the grounds that the legislation did respect privacy rights and included the necessary oversight measures to prevent abuses.

This demonstrates why the balance between security and privacy so often seems to favour security over privacy: security is a rhetorical motif that claims-makers hold in high priority and the agreement about the importance of privacy allows state representatives to claim that new surveillance respect and even protect privacy rights. These well-established motifs cannot be used to construct truly innovative claims about privacy, nor do they allow privacy advocates to effectively refute the expansion of surveillance.

To better understand how the rhetorical motifs of security and privacy constrain claims made about lawful access or surveillance in general, researchers should test the effectiveness of alternative claims based on Hong's (2017) argument that security of life and security of way of life should be held to the same degree of importance, which could allow privacy advocates to break away from their "obligation" to protect citizens at the cost of their privacy rights, or Petronio's (2013) suggestion that privacy rights should be framed as a matter of ownership of information, which could be used to construct a more specific definition of privacy rights than the current rhetoric of oversight and protections. Introducing new motifs into the claims would create new constructions of privacy that might not be as vulnerable to the state's claims that the expansion of surveillance is harmless and necessary.

This project also raises questions about how Spector and Kitsuse's (1973) four-stage natural history, which explains how social problems are constructed when members of the public make claims about putative social conditions and how relevant institutions, such as the government, respond to those claims. The ongoing expansion of surveillance and security measures is a well-recognized trend (Lyon, 2003; Mathiesen, 2013), and there is some evidence, based on the fact that claims from external groups were introduced into parliamentary discussions several years after the Conservative government introduced Bill C-46 and Bill C-47, that claims made about the dangers of new technologies and the need for lawful access emerged from the government itself. Although government representatives are members of the public and can make original claims about social problems, they possess formal authority that allows them to directly take action in response to social problems instead of having to present their claims to another group. This creates a specific power dynamic between government representatives and other claims-makers, an issue that is particularly important because of the way surveillance

extends state power into citizens' private lives and affects the democratic relationship between the state and its citizens.

The data presented in this project does not allow for an in-depth study of this issue, as communications between the government and other claims-maker groups primarily focused on House and Senate committees. It is therefore possible that other groups contacted the government to present their claims about the dangers of new technologies, and that these claims are the reason why the government introduced new lawful access legislation in 2009.

To better understand the relationship between the government and other claims-makers – and to evaluate how the four-stage natural history model should be applied in practical contexts – future research should examine contacts between government representatives and other groups with a vested interest in surveillance or privacy. Knowing when these discussions took place and what was discussed would make it possible to determine if surveillance measure originated from government claims-makers or if it they were a response to claims made by other groups. This would establish the relationship between the government, other claims-maker groups, and the social problems of surveillance and privacy.

Additionally, this research would be useful to identify which claims-makers are involved in the rhetorical construction of privacy within the context of formal laws, and whose claims have more influence over policy development than others. This would lead to a greater understanding of how public groups such as privacy commissioners, police representatives, victims' advocates, or privacy advocates influence the government through their claims.

References

- Adams, G. B., Balfour, D. L., & Reed, G. E. (2006). Abu Ghraib, administrative evil, and moral inversion: The value of "putting cruelty first". *Public Administration Review*, 66(5), 680-693. <https://doi.org/10.1111/j.1540-6210.2006.00633.x>
- Agamben, G. (2004). *State of exception* (K. Attell, Trans.). Chicago: University of Chicago Press. <https://doi.org/10.7208/chicago/9780226009261.001.0001>
- Akdeniz, Y. (2002). Anonymity, democracy, and cyberspace. *Social Research*, 69(1), 223-237. <https://dx.doi.org/10.1353/sor.2002.0010>
- Albas, D. (2012, February 28). "Opposition Motion – Charter of Rights and Freedoms." Canada. Parliament. House of Commons. *Edited Hansard 146(85)*. 41st Parliament, 1st session. <https://www.ourcommons.ca/Content/House/411/Debates/085/HAN085-E.PDF>
- Ananian-Welsh, R. (2015). Preventative detention orders and the separation of judicial power. *University of New South Wales Law Journal*, 38(2), 756–791.
- Anderson, S. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 28. <https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6645300/JUST-EV28-E.PDF>
- André, G. (2009, October 27). "Loi sur les pouvoirs d'enquête au XXI^e siècle." Canada. Parliament. House of Commons. *Hansard révisé 144(101)*. 40th Parliament, 2nd session. <https://www.noscommunes.ca/Content/House/402/Debates/101/HAN101-F.PDF>
- Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence, Kansas: University of Kansas Press. <https://doi.org/10.1353/book.119494>

- Armstrong, H. L., & Forde, P. J. (2003). Internet anonymity practices in computer crime. *Information Management & Computer Security*, 11(5), 209–215.
<https://doi.org/10.1108/09685220310500117>
- Austin, L. M. (2012). Getting past privacy? Surveillance, the Charter, and the rule of law. *Canadian Journal of Law and Society*, 27(3), 381–398.
<https://doi.org/10.1017/s0829320100010565>
- Austin, L. M. (2015). Lawful Illegality: What Snowden has taught us about the legal infrastructure of the surveillance state. In M. Geist (Ed.), *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (pp. 103–126). University of Ottawa Press.
<https://doi.org/10.2307/j.ctt15nmj3c.8>
- Axelrod, P. (1995). Spying on the young in depression and war: Students, youth groups and the RCMP, 1935-1942. *Labour / Le Travail*, 35, 43–63. <http://www.jstor.org/stable/25143911>
- Bailey, J. (2008). Framed by section 8: Constitutional protection of privacy in Canada. *Canadian Journal of Criminology & Criminal Justice*, 50(3), 279–306.
<https://doi.org/10.3138/cjccj.50.3.279>
- Baker, N. V. (2002). “The law”: The impact of antiterrorism policies on separation of powers: Assessing John Ashcroft’s role. *Presidential Studies Quarterly*, 32(4), 765–778.
<https://doi.org/10.1177/0360491802238708>
- Baker, N. V. (2003). National security versus civil liberties. *Presidential Studies Quarterly*, 33(3), 547–567. <https://doi.org/10.1111/1741-5705.00006>
- Ball, J. (2013, October 24). NSA monitored calls of 35 world leaders after US official handed over contact. *The Guardian*.
<http://www.theguardian.com/world/2013/oct/24/nsasurveillance- world-leaders-calls>

- Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity: The International Journal of Government & Democracy in the Information Age*, 10(1/2), 65–78. <https://doi.org/10.3233/ip-2005-0068>
- Baudrillard, J. (1994). *Simulation and simulacra* (S. F. Glaser, Trans.). United States of America: University of Michigan Press.
- Bentham, J., & Božovič, Miran. (1995). *The panopticon writings*. Verso.
- Best, J. (1987). Rhetoric in claims-making: Constructing the missing children problem. *Social Problems*, 34(2), 101-121. <https://doi.org/10.2307/800710>
- Best, J. (2003a). But seriously folks: The limitations of the strict constructionist interpretation of social problems. In J. A. Holstein and G. Miller (Eds.), *Challenges & choices* (1st edition, pp. 51-69). New York: Aldine de Gruyter.
- Best, J. (2003b). Staying alive: Prospects for constructionist theory. In J. A. Holstein and G. Miller (Eds.), *Challenges & choices* (1st edition, 133-152). New York: Aldine de Gruyter.
- Bigo, D., & Tsoukala, A. (2008) *Terror, insecurity and liberty: Illiberal practices of liberal regimes alter 9/11*. Routledge.
- Bill C-13, *An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Session, 41st Parliament, 2013. https://www.parl.ca/Content/Bills/412/Government/C-13/C-13_1/C-13_1.PDF
- Bill C-13, *An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Session, 41st Parliament, 2014. https://www.parl.ca/Content/Bills/412/Government/C-13/C-13_4/C-13_4.PDF
- Bill C-22, *An Act respecting lawful access*, 1st Session, 45th Parliament, 2026. https://www.parl.ca/Content/Bills/451/Government/C-22/C-22_1/C-22_1.PDF

Bill C-30, *An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts*, 1st Session, 41st Parliament, 2012.

https://www.parl.ca/Content/Bills/411/Government/C-30/C-30_1/C-30_1.PDF

Bill C-46, *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Session, 40th Parliament, 2009.

https://www.parl.ca/Content/Bills/402/Government/C-46/C-46_1/C-46_1.PDF

Bill C-47, *An Act regulating telecommunications facilities to support investigations*, 2nd Session, 40th Parliament, 2009. https://www.parl.ca/Content/Bills/402/Government/C-47/C-47_1/C-47_1.PDF

Bill C-50, *An Act to amend the Criminal Code (interception of private communications and related warrants and orders)*, 3rd Session, 40th Parliament, 2010.

https://www.parl.ca/Content/Bills/403/Government/C-50/C-50_1/C-50_1.PDF

Bill C-51, *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 3rd Session, 40th Parliament, 2010.

https://www.parl.ca/Content/Bills/403/Government/C-51/C-51_1/C-51_1.PDF

Bill C-52, *An Act regulating telecommunications facilities to support investigations*, 3rd Session, 40th Parliament, 2010. https://www.parl.ca/Content/Bills/403/Government/C-52/C-52_1/C-52_1.PDF

Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information*, 1st Session, 38th Parliament, 2005.

https://www.parl.ca/Content/Bills/381/Government/C-74/C-74_1/C-74_1.PDF

- Bockman, S. (1991). Interest, ideology, and claims-making activity. *Sociological Inquiry*, 61(4), 452-470. <https://doi.org/10.1111/j.1475-682x.1991.tb00173.x>
- Bogard, C. J. (2003). Explaining social problems: Addressing the whys of social Constructionism. In J. A. Holstein and G. Miller (Eds.), *Challenges & choices* (1st edition, pp. 209-235). New York: Aldine de Gruyter.
- Boisvenu, P.-H. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014). *Proceedings*. 41st Parliament, 2nd session, no. 21. <https://sencanada.ca/fr/content/sen/committee/412/lcjc/21ev-51748-f>
- Boivin, F. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 24. <https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6593964/JUST-EV24-E.PDF>
- Booth, N., Derefaka, G., Khan, R., & Brewer, G. (2023). Cyber intimate partner aggression in adulthood: The role of insecure attachment and self-control. *Journal of Criminal Psychology*, 13(4), 367-380. <https://doi.org/10.1108/JCP-03-2023-0015>
- Borg, C. (2013, November 28). "Protecting Canadians from Online Crime Act." Canada. Parliament. House of Commons. *Hansard révisé* 147(26). 41st Parliament, 2nd session. <https://www.noscommunes.ca/Content/House/412/Debates/026/HAN026-F.PDF>
- Brenner, S. W. (2006). Cybercrime jurisdiction. *Crime, Law and Social Change*, 46(4-5), 189-206. <https://doi.org/10.1007/s10611-007-9063-7>
- Brevini, B. (2017). Metadata laws, journalism and resistance in Australia. *Media and Communication*, 5(1), 76-83. <https://doi.org/10.17645/mac.v5i1.810>

- Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, 29(3), 408–433.
<https://doi.org/10.1108/13639510610684674>
- Brown, L., & Brown, C. (1978). *An unauthorized history of the RCMP* (1st edition). Toronto: James Lorimer
- Brown, M. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 26.
<https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6617624/JUST-EV26-E.PDF>
- Byman, D., & Wittes, B. (2014). Reforming the NSA: How to spy after Snowden. *Foreign Affairs* (New York, N.Y.), 93(3), 127–138.
<https://www.proquest.com/magazines/reforming-nsa-how-spy-after-snowden/docview/1520424083/se-2>
- Calderoni, F. (2010). The European legal framework on cybercrime: Striving for an effective implementation. *Crime, Law and Social Change*, 54(5), 339–357.
<https://doi.org/10.1007/s10611-010-9261-6>
- Calo, R. (2016). Can Americans resist surveillance? *The University of Chicago Law Review*, 83(1), 23–43. <https://www.jstor.org/stable/43741590>
- Campbell, C. (2005, October 11). Ottawa demands greater wiretap access. *The Globe and Mail*. <https://www.proquest.com/newspapers/ottawa-demands-greater-wiretap-access/docview/383611525/se-2>

Canadian Association of Chiefs of Police. (n.d.) *Simplying lawful access – Bill C-30 – Through the lens of law enforcement*. <https://www.publicsafety.gc.ca/lbrr/archives/cnmcs-pleng/cn31164-eng.pdf>

Canadian Charter of Rights and Freedoms, s 8, Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

Canning, G. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 24. <https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6593964/JUST-EV24-E.PDF>

Carmichael, J. (2013, November 28). “Protecting Canadians from Online Crime Act.” Canada. Parliament. House of Commons. *Edited Hansard 147(26)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/412/Debates/026/HAN026-E.PDF>

Casey, S. (2013, November 27). “Protecting Canadians from Online Crime Act.” Canada. Parliament. House of Commons. *Edited Hansard 147(25)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/412/Debates/016/HAN016-E.PDF>

Cash, A. (2013, November 28). “Protecting Canadians from Online Crime Act.” Canada. Parliament. House of Commons. *Edited Hansard 147(26)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/412/Debates/026/HAN026-E.PDF>

Cavoukian, A. (2012a, December 07). Misleading info about privacy (II). *National Post*. <https://www.proquest.com/newspapers/misleading-info-about-privacy-ii/docview/1223789432/se-2>

- Cavoukian, A. (2012b, December 03). The right to remain anonymous. *National Post*. <https://www.proquest.com/newspapers/right-remain-anonymous/docview/1222169316/se-2>
- Chaikin, D. (2006). Network investigations of cyber attacks: The limits of digital evidence. *Crime, Law and Social Change*, 46(4-5), 239-256.
<https://doi.org/10.1007/s10611-007-9058-4>
- Chetty, K. (2016). Persona designata, punitive purposes and the issue of preventative detention orders: All roads lead to infringement of the separation of judicial power. *Melbourne University Law Review*, 40(1), 87–125.
- Chu, J. (2012a, December 06). Misleading info about privacy bill. *National Post*. <https://www.proquest.com/newspapers/misleading-info-about-privacy-bill/docview/1223623071/se-2>
- Chu, J. (2012b, November 10). Privacy risk misunderstood. *Edmonton Journal*. <https://www.proquest.com/newspapers/privacy-risk-misunderstood/docview/1151224111/se-2>
- Chu, J. (2012c, November 05). New law is about safety, not about snooping. *Calgary Herald*. <https://www.proquest.com/newspapers/new-law-is-about-safety-not-snooping/docview/1140851281/se-2>
- Chu, J. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014a). *Evidence*. 41st Parliament, 2nd session, meeting no. 25.
<https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6606569/JUST-EV25-E.PDF>

- Chu, J. Canada. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014b). *Proceedings*. 41st Parliament, 2nd session, no. 20.
<https://sencanada.ca/en/content/sen/committee/412/lcjc/20ev-51714-e>
- Clarke, R. (2009, October 26). “Investigative Powers for the 21st Century Act.” Canada. Parliament. House of Commons. *Edited Hansard 144(100)*. 40th Parliament, 2nd session.
<https://www.ourcommons.ca/Content/House/402/Debates/100/HAN100-E.PDF>
- Clayton, J., Denham, E., & Cavoukian, A. (2012, November 07). Bill threatens our privacy. *Edmonton Journal*. <https://www.proquest.com/newspapers/bill-threatens-our-privacy/docview/1148949234/se-2>
- Clough, J. (2012). The Council of Europe Convention on Cybercrime: Defining ‘crime’ in a digital world. *Criminal Law Forum*, 23(4), 363-391. <https://doi.org/10.1007/s10609-012-9183-3>
- Comartin, J. (2009, October 29). “Technical Assistance for Law Enforcement in the 21st Century Act.” Canada. Parliament. House of Commons. *Edited Hansard 144(103)*. 40th Parliament, 2nd session.
<https://www.ourcommons.ca/Content/House/402/Debates/103/HAN103-E.PDF>
- Convention on Cybercrime, November 23, 2001,
<https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf>
- Convention Télégraphique Internationale de Paris, May 17, 1865,
<https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.1.43.fr.200.pdf>
- Côté, A. (2016). Agents without agency: Assessing the role of the audience in securitization theory. *Security Dialogue*, 47(6), 541–558. <https://doi.org/10.1177/0967010616672150>

Criminal Code, RSC 1985, c C - 46.

Crosby, A., & Monaghan, J. (2016). Settler colonialism and the policing of Idle No More. *Social Justice*, 43(2 (144)), 37–57. <http://www.jstor.org/stable/26380302>

Crowther, B. T. (2012). (Un)reasonable expectation of digital privacy. *Brigham Young University Law Review*, 2012(1), 343-369. <https://www.proquest.com/scholarly-journals/un-reasonable-expectation-digital-privacy/docview/929419489/se-2>

Davies, D. (2009, October 27). “Investigative Powers for the 21st Century Act.” Canada. Parliament. House of Commons. *Edited Hansard 144(101)*. 40th Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/402/Debates/101/HAN101-E.PDF>

Dechert, B. (2014a, September 22). “Motions in Amendment.” Canada. Parliament. House of Commons. *Edited Hansard 147(113)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/412/Debates/113/HAN113-E.PDF>

Dechert, B. (2014b, June 13). “Privacy.” Canada. Parliament. House of Commons. *Edited Hansard 147(103)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/412/Debates/103/HAN103-E.PDF>

Deleuze, G. (1995). *Negotiations, 1972-1990*. New York: Columbia University Press.

Denham, E., Cavoukian, A., & Clayton, J. (2012, Nov 14). Privacy rights do not restrict access to data in an emergency. *The Vancouver Sun*. <https://www.proquest.com/newspapers/privacy-rights-do-not-restrict-access-data/docview/1155936350/se-2>

Desai, A. C. (2007). Wiretapping before the wires: The post office and the birth of communications privacy. *Stanford Law Review*, 60(2), 553-594. Retrieved from

<https://www.proquest.com/scholarly-journals/wiretapping-before-wires-post-office-birth/docview/224070669/se-2>

Donnelly, F. (2013, November 28). "Protecting Canadians from Online Crime Act." Canada.

Parliament. House of Commons. *Edited Hansard 147(26)*. 41st Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/412/Debates/026/HAN026-E.PDF>

Dufour, N. (2009, October 27). "Loi sur les pouvoirs d'enquête au XXI^e siècle." Canada.

Parliament. House of Commons. *Hansard révisé 144(101)*. 40th Parliament, 2nd session.

<https://www.noscommunes.ca/Content/House/402/Debates/101/HAN101-F.PDF>

Durkheim, E. (1967). *Les règles de la méthode sociologique* (16th edition). Les Presses

Universitaires de France.

Durkheim, E. (1984). *The division of labor in society*. Free Press.

Easter, W. (2014a, October 1). "Protecting Canadians from Online Crime Act." Canada.

Parliament. House of Commons. *Edited Hansard 147(120)*. 41st Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/412/Debates/120/HAN120-E.PDF>

Easter, W. (2014b, Oct. 10). "Protecting Canadians from Online Crime Act." Canada. Parliament.

House of Commons. *Edited Hansard 147(127)*. 41st Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/412/Debates/127/HAN127-E.PDF>

Egawhary, E. M. (2019). The surveillance dimensions of the use of social media by UK police

forces. *Surveillance & Society*, 17(1/2), 89–104.

<https://doi.org/10.24908/ss.v17i1/2.12916>

- Eggstein, J. V., & Knapp, K. J. (2014). Fighting child pornography: A review of legal and technological developments. *The Journal of Digital Forensics, Security and Law: JDFSL*, 9(4), 29-48. <https://doi.org/10.15394/jdfsl.2014.1191>
- Etter, B. (2001, September 1). *The forensic challenges of e-crime*. Paper presented at the 7th Indo-Pacific Congress on Legal Medicine and Forensic Sciences, Melbourne.
- Fairall, P., & Lacey, W. (2007). Preventative detention and control orders under federal law: The case for a bill of rights. *Melbourne University Law Review*, 31(3), 1072–1098.
- Faqir, R. S. A. (2023). Digital criminal investigations in the era of artificial intelligence: A comprehensive overview. *International Journal of Cyber Criminology*, 17(2), 77-94.
- Finley, L., & Esposito, L. (2014). "Digital Blackwater": The National Security Administration, telecommunications companies and state-corporate crime. *State Crime*, 3(2), 182-199. <https://doi.org/10.13169/statecrime.3.2.0182>
- Finn, J. (2005). Potential threats and potential criminals: Data collection in the National Security Entry-Exit Registration System. In E. Zureik & M. Salter (Eds.), *Global surveillance and policing borders, security, identity* (pp. 139-156). Cullompton: Willan.
- Fitzpatrick, W. M., & DiLullo, S. A. (2013). International trade secret protection: Global issues and responses. *Competition Forum*, 11(2), 21-46.
- Flyvbjerg, B. (2001). *Making social science matter: Why social inquiry fails and how it can succeed again*. New York: Cambridge University Press.
- Foote, J. (2012, February 28). "Opposition Motion – Charter of Rights and Freedoms." Canada. Parliament. House of Commons. *Edited Hansard 146(85)*. 41st Parliament, 1st session. <https://www.ourcommons.ca/Content/House/411/Debates/085/HAN085-E.PDF>

- Foucault, M. (1995). *Discipline and punish*. Toronto: Random House Canada Limited.
- Fox, W., Coupland, S., & Hart, S. (2024). Online stalking of Instagram influencers. *Journal of Threat Assessment and Management*, 11(4), 229-247. <https://doi.org/10.1037/tam0000226>
- Fraser, D. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 22. <https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6573637/JUST-EV22-E.PDF>
- Frum, L. Canada. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014a). *Proceedings*. 41st Parliament, 2nd session, no. 21. <https://sencanada.ca/en/content/sen/committee/412/lcjc/21ev-51748-e>
- Frum, L. Canada. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014b). *Proceedings*. 41st Parliament, 2nd session, no. 21. <https://sencanada.ca/en/content/sen/committee/412/lcjc/21ev-51760-e>
- Fuchs, C., & Trottier, D. (2017). Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the internet and social media post-Edward Snowden. *Journal of Information, Communication & Ethics in Society*, 15(4), 412-444. <https://doi.org/10.1108/JICES-01-2016-0004>
- Fuller, R. C., & Myers, R. R. (1941a). Some aspects of a theory of social problems. *American Sociological Review*, 6(1), 24-32. <https://doi.org/10.2307/2086338>
- Fuller, R. C., & Myers, R. R. (1941b). The natural history of a social problem. *American Sociological Review*, 6(3), 320-329. <https://doi.org/10.2307/2086189>

- Gao, R. Y. (2025). Forum shifting to regulate data privacy: The creation and evolution of EU data protection law. *Northwestern Journal of International Law & Business*, 45(3), 329-418. <https://doi.org/10.2139/ssrn.5337206>
- Geist, M. A. (2001). *Internet law in Canada* (2nd edition). Captus Press.
- Geist, M. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014a). *Evidence*. 41st Parliament, 2nd session, meeting no. 27. <https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6632973/JUSTEV27-E.PDF>
- Geist, M. Canada. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014b). *Proceedings*. 41st Parliament, 2nd session, no. 21. <https://sencanada.ca/en/content/sen/committee/412/lcjc/21ev-51748-e>
- Genest-Jourdain, J. (2013, November 28). “Loi sur la Protection des Canadiens contre la Cybercriminalité.” Canada. Parliament. House of Commons. *Edited Hansard 147(27)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/412/Debates/026/HAN026-E.PDF>
- Gilhooly, G. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014a). *Evidence*. 41st Parliament, 2nd session, meeting no. 26. <https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6617624/JUSTEV26-E.PDF>
- Gilhooly, G. Canada. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014b). *Proceedings*. 41st Parliament, 2nd session, no. 20. <https://sencanada.ca/en/content/sen/committee/412/lcjc/20ev-51725-e>

- Glac, K., Elm, D. R., & Martin, K. (2014). Areas of privacy in Facebook: Expectations and value. *Business & Professional Ethics Journal*, 33(2/3), 147–176.
<https://doi.org/10.5465/ambpp.2013.12892abstract>
- Glennon, M. J. (2012). State-level cybersecurity. *Policy Review*, (171), 85-102. Retrieved from
<http://search.proquest.com/docview/921993402>
- Glover, G. (2009, October 27). “Technical Assistance for Law Enforcement in the 21st Century Act.” Canada. Parliament. House of Commons. *Edited Hansard 144(101)*. 40th Parliament, 2nd session.
<https://www.ourcommons.ca/Content/House/402/Debates/101/HAN101-E.PDF>
- Godfrey, M., & Simbarashe, G. (2025). Youth politics of engagement and resistance: Agency on social media spaces in contexts of crisis. *Journal of Asian and African Studies*, 60(4), 2120-2134. <https://doi.org/10.1177/00219096231207883>
- Goguen, R. (2014, October 10). “Protecting Canadians from Online Crime Act.” Canada. Parliament. House of Commons. *Edited Hansard 147(127)*. 41st Parliament, 2nd session.
<https://www.ourcommons.ca/Content/House/412/Debates/127/HAN127-E.PDF>
- Guthrie, S. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 22.
<https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6573637/JUST-EV22-E.PDF>
- Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology*, 51(4), 605-622. <https://doi.org/10.1080/00071310020015280>

- Hagmann, J., Hegemann, H., & Neal, A. (2018). The politicisation of security: Controversy, mobilisation, arena shifting. *European Review of International Studies*, 5(3), 3–29.
<https://doi.org/10.3224/eris.v5i3.01>
- Hanniman, W. (2008). Canadian Muslims, Islamophobia and national security. *International Journal of Law, Crime and Justice*, 36(4), 271–285.
<https://doi.org/10.1016/j.ijlcj.2008.08.003>
- Harris, J. (2012, February 28). “Opposition Motion – Charter of Rights and Freedoms.” Canada. Parliament. House of Commons. *Edited Hansard 146(85)*. 41st Parliament, 1st session.
<https://www.ourcommons.ca/Content/House/411/Debates/085/HAN085-E.PDF>
- Helms, M. M., Ettkin, L. P., & Morris, D. J. (2000). IN-security: The pillaging of corporate America. *Competitive Intelligence Review*, 11(3), 93–106. [https://doi.org/10.1002/1520-6386\(200033\)11:3<93::AID-CIR10>3.0.CO;2-K](https://doi.org/10.1002/1520-6386(200033)11:3<93::AID-CIR10>3.0.CO;2-K)
- Hills, J. (2006). What's new? War, censorship and global transmission: From the telegraph to the internet. *The International Communication Gazette*, 68(3), 195–216.
<https://doi.org/10.1177/1748048506063761>
- Hoback, R. (2014, April 28). “Protecting Canadians from Online Crime Act.” Canada. Parliament. House of Commons. *Edited Hansard 147(75)*. 41st Parliament, 2nd session.
<https://www.ourcommons.ca/Content/House/412/Debates/202/HAN202-E.PDF>
- Hochman, Brian. (2022). *The listeners: A history of wiretapping in the United States*. Harvard University Press. <https://doi.org/10.4159/9780674275720>
- Holland, M. (2009a, October 26). “Investigative Powers for the 21st Century Act.” Canada. Parliament. House of Commons. *Edited Hansard 144(100)*. 40th Parliament, 2nd session.
<https://www.ourcommons.ca/Content/House/402/Debates/100/HAN100-E.PDF>

- Holland, M. (2009b, October 27). "Technical Assistance for Law Enforcement in the 21st Century Act." Canada. Parliament. House of Commons. *Edited Hansard 144(101)*. 40th Parliament, 2nd session.
<https://www.ourcommons.ca/Content/House/402/Debates/101/HAN101-E.PDF>
- Hollway, W., & Jefferson, T. (1997). The risk society in an age of anxiety: Situating fear of crime. *The British Journal of Sociology*, 48(2), 255–266. <https://doi.org/10.2307/591751>
- Holstein, J. A., & Gubrium, J. F. (2013). A constructionist analytics for social problems. In J. A. Holstein & G. Miller (Eds.), *Challenges & choices* (1st ed., pp. 187-208). New York: Aldine de Gruyter. <https://doi.org/10.4324/9781003571841-11>
- Holstein, J. A., & Miller, G. (2013). Social constructionism and social problems work. In J. A. Holstein & G. Miller (Eds.), *Challenges & choices* (1st ed., pp. 70-91). New York: Aldine de Gruyter. <https://doi.org/10.4324/9781003571841-5>
- Hong, H., & Kim, Y. (2021). What makes people engage in civic activism on social media? *Online Information Review*, 45(3), 562-576. <https://doi.org/10.1108/OIR-03-2020-0105>
- Hong, S. (2017). Criticising surveillance and surveillance critique: Why privacy and humanism are necessary but insufficient. *Surveillance & Society*, 15(2), 187–203.
<https://doi.org/10.24908/ss.v15i2.5441>
- Howe, M., & Monaghan, J. (2018). Strategic incapacitation of Indigenous dissent: Crowd theories, risk management, and settler colonial policing. *The Canadian Journal of Sociology / Cahiers Canadiens de Sociologie*, 43(4), 325–348.
<https://doi.org/10.29173/cjs29397>
- Huey, L., & Rosenberg, R. (2004). 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.
<https://doi.org/10.3138/cjccj.46.5.597>
- Hunter et al. v. Southam Inc., 1984 S.C.R. 145. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/5274/index.do>
- Huq, A. Z., Jackson, J., & Trinker, R. (2017). Legitimizing practices: Revisiting the predicates of police legitimacy. *British Journal of Criminology*, 57(5), 1101–1122.
<https://doi.org/10.1093/bjc/azw037>
- Ibarra, P. R., & Kitsuse, J. I. (2003). Claimsmaking Discourse and Vernacular Resources. In J. A. Holstein and G. Miller (Eds.), *Challenges & Choices* (1st ed., pp. 17-50). New York: Aldine de Gruyter.
- Ibarra, P. R., Kitsuse, J. I. (1993). “Vernacular Constituents of Moral Discourse: An Interactionist Proposal for the Study of Social Problems”, in Holstein, J.A. & Miller, G. (Eds.), *Reconsidering Social Constructionism: Debates in Social Problems Theory* (pp. 25-58). New York: Aldine De Gruyter.
- Jackson, J., & Gray, E. (2010). Functional fear and public insecurities about crime. *The British Journal of Criminology*, 50(1), 1–22. <https://doi.org/10.1093/bjc/azp059>
- Jackson, J., Bradford, B., Hough, M., Myhill, A., Quinton, P., & Tyler, T. (2012). Why do people comply with the law? Legitimacy and the influence of legal institutions. *The British Journal of Criminology*, 52(6), 1051-1071. <https://doi.org/10.2139/ssrn.1994490>
- Jamil, U. (2017). Can Muslims fly? The no fly list as a tool of the “War on Terror.” *Islamophobia Studies Journal*, 4(1), 72–86. <https://doi.org/10.13169/islastudj.4.1.0072>

- Joyal, S. Canada. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014). *Proceedings*. 41st Parliament, 2nd session, no. 21.
<https://sencanada.ca/en/content/sen/committee/412/lcjc/21ev-51748-e>
- Jurich, J. P. (2008). Cyberwar and customary international law: The potential of a "bottom-up" approach to an international law of information operations. *Chicago Journal of International Law*, 9(1), 275-295. <http://search.proquest.com/docview/237217859>
- Kamp, R. (2009, October 27). "Investigative Powers for the 21st Century Act." Canada. Parliament. House of Commons. *Edited Hansard 144(101)*. 40th Parliament, 2nd session.
<https://www.ourcommons.ca/Content/House/402/Debates/101/HAN101-E.PDF>
- Kealey, G. S. (1992). The RCMP, the special branch, and the early days of the Communist Party of Canada: A documentary article. *Labour / Le Travail*, 30, 169–204.
<https://doi.org/10.2307/25143626>
- Kelly, N. (2022). Facing surveillance: Personified surveillance, algorithmic injustice, and the myth of Big Brother in post-Snowden popular culture. *Surveillance & Society*, 20(2), 172-185. <https://doi.org/10.24908/ss.v20i2.14492>
- Kinsman, G. (1995). "Character weaknesses" and "fruit machines": Towards an analysis of the anti-homosexual security campaign in the Canadian civil service. *Labour / Le Travail*, 35, 133–161. <https://doi.org/10.2307/25143914>
- Kitsuse, J. I., & Spector, M. (1973). Toward a sociology of social problems: social conditions, value-judgments, and social problems. *Social Problems*, 20(4), 407-419.
<https://doi.org/10.1525/sp.1973.20.4.03a00020>
- Kitsuse, J. I., & Spector, M. (1975). Social problems and deviance: Some parallel issues. *Social Problems*, 22(1), 584-594. <https://doi.org/10.1525/sp.1975.22.5.03a00040>

Krebs, R., & Lobasz, J. (2007). Fixing the meaning of 9/11: Hegemony, coercion, and the road to war in Iraq. *Security Studies*, 16(3), 409–451.

<https://doi.org/10.1080/09636410701547881>

Lamoureux, K. (2014, April 28). “Protecting Canadians from Online Crime Act.” Canada.

Parliament. House of Commons. *Edited Hansard 147(75)*. 41st Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/412/Debates/202/HAN202-E.PDF>

Lashmar, P. (2017). No More Sources? The impact of Snowden’s revelations on journalists and their confidential sources. *Journalism Practice*, 11(6), 665–688.

<https://doi.org/10.1080/17512786.2016.1179587>

Leblanc, D. (2014, October 1). “Protecting Canadians from Online Crime Act.” Canada.

Parliament. House of Commons. *Edited Hansard 147(120)*. 41st Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/412/Debates/120/HAN120-E.PDF>

Leef, R. (2014, October 10). “Protecting Canadians from Online Crime Act.” Canada.

Parliament. House of Commons. *Edited Hansard 147(127)*. 41st Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/412/Debates/127/HAN127-E.PDF>

Lefebvre, R. D. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 31.

<https://www.noscommunes.ca/Content/Committee/412/JUST/Evidence/EV6670175/JUS-TEV31-F.PDF>

Lentz, C. E. (2010). A state's duty to prevent and respond to cyberterrorist acts. *Chicago Journal of International Law*, 10(2), 799-823. Retrieved from

<http://search.proquest.com/docview/237213322>

- LeRat, H., & Ungar, L. (2021). *Treaty promises, Indian reality: Life on a reserve*. Purich Publishing Limited.
- Lessig, L. (1999b). The limits in open code: Regulatory standards and the future of the net. *Berkeley Technology Law Journal*, 14(2), 759-769. Retrieved from <https://www.proquest.com/scholarly-journals/limits-open-code-regulatory-standards-future-net/docview/204769321/se-2>
- Lessig, L. (1999). The Architecture of Privacy. *Vanderbilt Journal of Entertainment Law & Practice*, 1, 56-65. <https://heinonline.org/HOL/P?h=hein.journals/vanep1&i=58>
- Lirëza, L., & Koçi, G. (2023). Child cyberpornography in EU countries: The ways of protecting children's integrity. *Perspectives of Law and Public Administration*, 12(2), 230-237. Retrieved from <https://www.proquest.com/scholarly-journals/child-cyberpornography-eu-countries-ways/docview/2834503882/se-2>
- Livingstone, S., & Bober, M. (2003). *UK children go online: Listening to young people's experiences. Technical Report*. London School of Economics and Political Science, London, UK.
- Lonardo, M. (1995). Under a watchful eye: A case study of police surveillance during the 1930s. *Labour / Le Travail*, 35, 11-41. <https://doi.org/10.2307/25143910>
- Lyon, D. (2003). *Surveillance after September 11*. Cambridge: Polity.
- Maas, W. (2005). Freedom of movement inside 'Fortress Europe'. In E. Zureik & M. Salter (Eds.), *Global surveillance and policing borders, security, identity* (pp. 233-246). Cullompton: Willan.

- MacKay, P. (2013, November 27). “Protecting Canadians from Online Crime Act.” Canada. Parliament. House of Commons. *Edited Hansard 147(25)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/412/Debates/016/HAN016-E.PDF>
- MacKay, P. (2014a, October 1). “Protecting Canadians from Online Crime Act.” Canada. Parliament. House of Commons. *Edited Hansard 147(120)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/412/Debates/120/HAN120-E.PDF>
- MacKay, P. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014b). *Evidence*. 41st Parliament, 2nd session, meeting no. 21. <https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6557203/JUST-EV21-E.PDF>
- MacKenzie, D. (2012, February 28). “Opposition Motion – Charter of Rights and Freedoms.” Canada. Parliament. House of Commons. *Edited Hansard 146(85)*. 41st Parliament, 1st session. <https://www.ourcommons.ca/Content/House/411/Debates/085/HAN085-E.PDF>
- MacLeod, C. (2014, October 10). “Protecting Canadians from Online Crime Act.” Canada. Parliament. House of Commons. *Edited Hansard 147(127)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/412/Debates/127/HAN127-E.PDF>
- Maguire, L. (2014, April 28). “Protecting Canadians from Online Crime Act.” Canada. Parliament. House of Commons. *Edited Hansard 147(75)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/412/Debates/075/HAN075-E.PDF>
- Maloway, J. (2009, October 29). “Technical Assistance for Law Enforcement in the 21st Century Act.” Canada. Parliament. House of Commons. *Edited Hansard 144(103)*. 40th

Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/402/Debates/103/HAN103-E.PDF>

Marit, A., Şargu, L., & Corsei, A. (2022). The impact of the use of information technologies (ICT) on minors and children through online sexual abuse and exploitation. *Euromentor Journal*, 13(1), 66-89. <https://www.proquest.com/scholarly-journals/impact-use-information-technologies-ict-on-minors/docview/2647406718/se-2>

Marster, W. (2014, September 22). “Motions in Amendment.” Canada. Parliament. House of Commons. *Edited Hansard 147(113)*. 41st Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/412/Debates/113/HAN113-E.PDF>

Martin, K. E. (2012). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics*, 111(4), 519–539.

<https://doi.org/10.1007/s10551-012-1215-8>

Mathiesen, T. (2013). *Towards a surveillant society: The rise of surveillance systems in Europe*. United Kingdom: Waterside Press.

Mazerolle, L., Antrobus, E., Bennett, S., & Tyler, T. R. (2013). Shaping citizen perceptions of police legitimacy: A randomized field trial of procedural justice. *Criminology*, 51(1), 33–63. <https://doi.org/10.1111/j.1745-9125.2012.00289.x>

McColeman, P. (2009, October 27). “Technical Assistance for Law Enforcement in the 21st Century Act.” Canada. Parliament. House of Commons. *Edited Hansard 144(101)*. 40th Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/402/Debates/101/HAN101-E.PDF>

- McInnis, T. J. Canada. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014). *Proceedings*. 41st Parliament, 2nd session, no. 21. <https://sencanada.ca/en/content/sen/committee/412/lcjc/21ev-51760-e>
- McQuillan, D. (2022). *Resisting AI: An anti-fascist approach to artificial intelligence*. Bristol University Press: Bristol, UK.
- Merton, R. K., & Nisbet, R. A. (1971). *Contemporary Social Problems* (3rd Revised Edition). New York: Harcourt, Brace and World.
- Mladenov, M., & Galetin, M. (2025). The unbreakable code shaping digital resistance: A right to encryption in the jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union. *Juridical Tribune - Review of Comparative and International Law*, 15(3), 578-591.
- Molinaro, D. (2017). “In the field of espionage, there’s no such thing as peacetime”: The official secrets act and the picnic wiretapping program. *Canadian Historical Review*, 98(3), 457–482. <https://doi.org/10.3138/chr.4220>
- Monaghan, J. (2013). Settler governmentality and racializing surveillance in Canada’s North-West. *Canadian Journal of Sociology*, 38(4), 487–508. <https://doi.org/10.29173/cjs21195>
- Monaghan, J., & Walby, K. (2012). Making up “Terror Identities”: Security intelligence, Canada’s Integrated Threat Assessment Centre and social movement suppression. *Policing & Society*, 22(2), 133–151. <https://doi.org/10.1080/10439463.2011.605131>
- Moore, A. D. (2011). Privacy, security, and government surveillance: Wikileaks and the new accountability. *Public Affairs Quarterly*, 25(2), 141–156. <https://www.jstor.org/stable/23057094>

- Moule, R. K. Jr, Parry, M. M., Burruss, G. W., & Fox, B. (2019). Assessing the direct and indirect effects of legitimacy on public empowerment of police: A study of public support for police militarization in America. *Law & Society Review*, 53(1), 77-107.
<https://doi.org/10.1111/lasr.12379>
- Nagra, B., & Maurutto, P. (2016). Crossing borders and managing racialized identities: Experiences of security and surveillance among young Canadian Muslims. *The Canadian Journal of Sociology / Cahiers Canadiens de Sociologie*, 41(2), 165–194.
<https://doi.org/10.29173/cjs23031>
- Nantel, P. (2013, November 28). “Loi sur la Protection des Canadiens contre la Cybercriminalité.” Canada. Parliament. House of Commons. *Hansard révisé* 147(27). 41st Parliament, 2nd session.
<https://www.noscommunes.ca/Content/House/412/Debates/026/HAN026-F.PDF>
- Nasu, H. (2015). State secrets law and national security. *The International and Comparative Law Quarterly*, 64(2), 365-404. <http://dx.doi.org/10.1017/S0020589315000056>
- Naylor, S. Canada. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014). *Proceedings*. 41st Parliament, 2nd session, no. 20.
<https://sencanada.ca/en/content/sen/committee/412/lcjc/20ev-51725-e>
- Neocleous, M. (2006). The problem with normality: Taking exception to “permanent emergency”. *Alternatives: Global, Local, Political*, 31(2), 191-213.
<https://doi.org/10.1177/030437540603100204>

- Neocleous, M. (2007). Security, liberty and the myth of balance: Towards a critique of security politics. *Contemporary Political Theory*, 6(2), 131-149.
<https://doi.org/10.1057/palgrave.cpt.9300301>
- Nyst, C. (2018). Secrets and lies: The proliferation of state surveillance capabilities and the legislative secrecy which fortifies them – An activist's account. *State Crime Journal*, 7(1), 8–23. <https://doi.org/10.13169/statecrime.7.1.0008>
- O'Brien, K., A. (2009). Managing national security and law enforcement intelligence in a globalised world. *Review of International Studies*, 35(4), 903-915.
<http://dx.doi.org/10.1017/S0260210509990349>
- Office of the Privacy Commissioner of Canada. (2013). *What an IP address can reveal about you: A report prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada*. https://www.priv.gc.ca/media/1767/ip_201305_e.pdf
- Ogasawara, M. (2022). Legalizing illegal mass surveillance: A transnational perspective on Canada's legislative response to the expansion of security intelligence. *Canadian Journal of Law and Society*, 37(2), 317-338. <https://doi.org/10.1017/cls.2022.9>
- Oliver, J. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 25.
[https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6606569/JUST EV25-E.PDF](https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6606569/JUST%20EV25-E.PDF)
- Pallaras, S. (2011). New technology: opportunities and challenges for prosecutors. *Crime, Law and Social Change*, 56(1), 71-89. <http://dx.doi.org/10.1007/s10611-011-9300-y>

- Pandey, V., Gupta, S., & Chattopadhyay, M. (2020). A framework for understanding citizens' political participation in social media. *Information Technology & People*, 33(4), 1053-1075. <https://doi.org/10.1108/ITP-03-2018-0140>
- Pardy, C. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 25. [https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6606569/JUST EV25-E.PDF](https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6606569/JUST%20EV25-E.PDF)
- Parnaby, A., & Kealey, G. S. (1997). How the “Reds” got their man: The Communist Party Unmasks an RCMP spy. *Labour / Le Travail*, 40, 253–259. <https://doi.org/10.2307/25144171>
- Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.
- Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, 13(1), 6-14. <http://dx.doi.org/10.1080/15267431.2013.743426>
- Pozen, D. E. (2016). Privacy-privacy tradeoffs. *The University of Chicago Law Review*, 83(1), 221–247. <https://www.jstor.org/stable/43741598>
- Privacy Act*, RSC 1985, c P- 21.
- ProQuest. (n.d.). *Basic search – Canadian major dailies – ProQuest*. <https://www.proquest.com/canadiannews/major>
- Proulx, C. (2014). Colonizing surveillance: Canada constructs an Indigenous terror threat. *Anthropologica*, 56(1), 83–100. <http://www.jstor.org/stable/24469643>
- Public Safety Canada. (n.d.) *Myths and facts about Protecting Children from Internet Predators Act* (Office of the Privacy Commissioner of Canada ATIP Request No. A-2013-00264).

R. v. Edwards, [1996] 1 S.C.R. 128. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1340/index.do>

R. v. Dymont, [1988] 2 S.C.R. 417. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/375/index.do>

R. v. Evans, [1996] 1 S.C.R. 8. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1333/index.do>.

R. v. Plant, [1993] 3 S.C.R. 281. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/1049/index.do>

R. v. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/14233/index.do>

R. v. Tessling, [2004] 3 S.C.R. 432, 2004 SCC 67. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/2183/index.do>

R. v. Thompson, [1990] 2 S.C.R. 1111. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/667/index.do>

Rathgeber, B. (2009, October 27). “Investigative Powers for the 21st Century Act.” Canada. Parliament. House of Commons. *Edited Hansard 144(101)*. 40th Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/402/Debates/101/HAN101-E.PDF>

Restivo, K. (2002, August 30). Ottawa mulls tracking Internet usage: Law enforcement powers: [National edition]. *National Post*. <https://www.proquest.com/newspapers/ottawa-mulls-tracking-internet-usage-law/docview/330124412/se-2>

- Rohret, D. M., & Kraft, M. E. (2011). Catch me if you can: Cyber anonymity. *Journal of Information Warfare*, 10(2), 11–21. <https://www.jstor.org/stable/26486804>
- Rozenshtein, A. Z. (2018). Surveillance intermediaries. *Stanford Law Review*, 70(1), 99-189. <https://www.proquest.com/scholarly-journals/surveillance-intermediaries/docview/3080762382/se-2>
- Russomanno, L. Canada. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014). *Proceedings*. 41st Parliament, 2nd session, no. 21. <https://sencanada.ca/en/content/sen/committee/412/lcjc/21ev-51748-e>
- Ryan, M. (2011). 'War in countries we are not at war with': The 'War on Terror' on the periphery from Bush to Obama. *International Politics, Suppl. Special Issue: American Power and Identities in the Age of*, 48(2-3), 364-389. <https://doi.org/10.1057/ip.2011.7>
- Sagar, R. (2015). Against moral absolutism: Surveillance and disclosure after Snowden. *Ethics & International Affairs*, 29(2), 145-159. <http://doi.org/10.1017/S0892679415000040>
- Sahill, P. H. (2019). The U.S. War on Terror discourse: Mapping de-politicization and the politics of confinement in Afghanistan. *Insight Turkey*, 21(1), 189-208. <https://doi.org/10.25253/99.2018211.13>
- Sandhu, J. (2012, February 28). “Opposition Motion – Charter of Rights and Freedoms.” Canada. Parliament. House of Commons. *Edited Hansard 146(85)*. 41st Parliament, 1st session. <https://www.ourcommons.ca/Content/House/411/Debates/085/HAN085-E.PDF>
- Scarpaleggia, F. (2012, February 13). “Public Safety.” Canada. Parliament. House of Commons. *Edited Hansard 146(79)*. 41st Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/411/Debates/079/HAN079-E.PDF>

- Schaaf, M., & Quiring, O. (2023). The limits of social media mobilization: How protest movements adapt to social media logic. *Media and Communication*, 11(3), 203-213. <https://doi.org/10.17645/mac.v11i3.6635>
- Scheffauer, R., Goyanes, M., & Gil de Zúñiga, H. (2021). Beyond social media news use algorithms: How political discussion and network heterogeneity clarify incidental news exposure. *Online Information Review*, 45(3), 633-650. <https://doi.org/10.1108/OIR-04-2020-0133>
- Scott, J. C., Tehranian, J., & Mathias, J. (2004). Government Surnames and Legal Identities. In Carl Watner and Wendy McElroy (Eds.), *National Identification Systems: Essays in Opposition* (pp. 11-55). McFarland.
- Scott, S. (2009, October 26). “Investigative Powers for the 21st Century Act.” Canada. Parliament. House of Commons. *Edited Hansard 144(100)*. 40th Parliament, 2nd session. <https://www.ourcommons.ca/Content/House/402/Debates/100/HAN100-E.PDF>
- Segal, M. D. (2015). *Independent review of the police and prosecution response to the Rehtaeh Parsons case*. <https://novascotia.ca/segalreport/Parsons-Independent-Review.pdf>
- Sgro, J. (2012, February 28). “Opposition Motion – Charter of Rights and Freedoms.” Canada. Parliament. House of Commons. *Edited Hansard 146(85)*. 41st Parliament, 1st session. <https://www.ourcommons.ca/Content/House/411/Debates/085/HAN085-E.PDF>
- Shade, L. R. (2008). Reconsidering the right to privacy in Canada. *Bulletin of Science, Technology & Society*, 28(1), 80-91. <http://dx.doi.org/10.1177/0270467607310591>

- Shillito, M. R. (2019). Untangling the “Dark Web”: An emerging technological challenge for the criminal law. *Information & Communications Technology Law*, 28(2), 186–207.
<https://doi.org/10.1080/13600834.2019.1623449>
- Sims, J. J. (2014, September 22). “Motions in Amendment.” Canada. Parliament. House of Commons. *Edited Hansard 147(113)*. 41st Parliament, 2nd session.
<https://www.ourcommons.ca/Content/House/412/Debates/113/HAN113-E.PDF>
- Slane, A. Canada. Parliament. Senate. Standing Senate Committee on Legal and Constitutional Affairs. (2014). *Proceedings*. 41st Parliament, 2nd session, no. 21.
<https://sencanada.ca/en/content/sen/committee/412/lcjc/21ev-51748-e>
- Smith, K. D. (2009). *Liberalism, surveillances and resistance: Indigenous communities in Western Canada, 1877-1927*. Athabasca University Press.
<https://www.fulcrum.org/concern/monographs/2r36v092r>
- Smith, L. N., & Hill, G. D. (1991). Perceptions of Crime Seriousness and Fear of Crime. *Sociological Focus*, 24(4), 315–327. <http://www.jstor.org/stable/20831596>
- Smith, T. M. (2012, March 8). Don't fear the 'inspector clause'. *National Post*. <https://www.proquest.com/newspapers/dont-fear-inspector-clause/docview/927065371/se-2>
- Smyth, S. M. (2012). The new social media paradox: A symbol of self-determination or a noon for Big Brother? *International Journal of Cyber Criminology*, 6(1), 924-950.
<https://www.proquest.com/scholarly-journals/new-social-media-paradox-symbol-self/docview/1077383753/se-2>

- Spector, M., & Kitsuse, J. I. (1973). Social problems: A re-formulation. *Social Problems*, 21(2), 145-159. <https://doi.org/10.2307/799536>
- Spector, M., & Kitsuse, J. I. (2017). *Constructing social problems* (1st edition). Taylor and Francis. <https://doi.org/10.4324/9781315080512>
- Speer, D. L. (2000). Redefining borders: The challenges of cybercrime. *Crime, Law and Social Change*, 34(3), 259-273.
<http://search.proquest.com/docview/216163304?accountid=14701>
- Spratt, M. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 26.
<https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6617624/JUST-EV26-E.PDF>
- St. Germain, M. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 27.
<https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6632973/JUST-EV27-E.PDF>
- Steeves, V. (2008). If the Supreme Court were on Facebook: Evaluating the reasonable expectation of privacy test from a social perspective. *Canadian Journal of Criminology and Criminal Justice/Revue Canadienne De Criminologie Et De Justice Penale*, 50(3), 331-348. <https://doi.org/10.3138/cjccj.50.3.331>
- Steeves, V., & Piñero, V. (2008). Privacy and police powers: Situating the reasonable expectation of privacy test. *Canadian Journal of Criminology and Criminal Justice*, 50(3), 263-278. <https://doi.org/10.3138/cjccj.50.3.263>

- Stoddart, J. (2012a, November 15). Modern privacy challenges. *The Ottawa Citizen*. <https://www.proquest.com/newspapers/modern-privacy-challenges/docview/1163484619/se-2>
- Stoddart, J. (2012b, November 8). Privacy laws need update too. *Edmonton Journal*. <https://www.proquest.com/newspapers/privacy-laws-need-update-too/docview/1150395216/se-2>
- Stonebanks, C. D. (2019). Secularism and securitisation: The imaginary threat of religious minorities in Canadian public spaces. *Journal of Beliefs and Values*, 40(3), 303–320. <https://doi.org/10.1080/13617672.2019.1600341>
- Therrien, D. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 30. <https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6662209/JUST-EV30-E.PDF>
- Thomas, N. (1994). *Colonialism's culture: Anthropology, travel, and government*. Princeton University Press.
- Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission), [1990] 1 S.C.R. 425. <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/583/index.do>
- Tigar, M. E. (2014). The national security state: The end of separation of powers. *Monthly Review*, 66(3), 136-159. <http://search.proquest.com/docview/1543483328?accountid=14701>

Todd, C. Canada. Parliament. House of Commons. Standing Committee on Justice and Human Rights. (2014). *Evidence*. 41st Parliament, 2nd session, meeting no. 24.

<https://www.ourcommons.ca/Content/Committee/412/JUST/Evidence/EV6593964/JUST-EV24-E.PDF>

Toews, V. (2012a, February 28). “Business of Supply.” Canada. Parliament. House of Commons. *Edited Hansard 146(79)*. 41st Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/411/Debates/085/HAN085-E.PDF>

Toews, V. (2012b, February 13). “Public Safety.” Canada. Parliament. House of Commons. *Edited Hansard 146(79)*. 41st Parliament, 2nd session.

<https://www.ourcommons.ca/Content/House/411/Debates/079/HAN079-E.PDF>

Toulmin, S., Rieke, R. and Janik, A. (1984). *An introduction to reasoning*. New York: Macmillian Publishing Company.

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies*, 18(4–5), 530–547.

<https://doi.org/10.1177/1367549415577396>

Tyler, T. R., & Huo, Y. J. (2002). *Trust in the law: Encouraging public cooperation with the police and courts through*. Russell Sage Foundation. <http://www.jstor.org/stable/10.7758/9781610445429>

Velasquez, A., & LaRose, R. (2015). Social media for social change: Social media political efficacy and activism in student activist groups. *Journal of Broadcasting & Electronic Media*, 59(3), 456–474. <https://doi.org/10.1080/08838151.2015.1054998>

Vogel, K. M., Reid, G., Kampe, C., & Jones, P. (2021). The impact of AI on intelligence analysis: Tackling issues of collaboration, algorithmic transparency, accountability, and

- management. *Intelligence and National Security*, 36(6), 827–848.
<https://doi.org/10.1080/02684527.2021.1946952>
- Wang, S., & Zhu, J. J. H. (2003). Mapping film piracy in China. *Theory, Culture & Society*, 20(4), 97–125. <https://doi.org/10.1177/02632764030204007>
- Weinberg, D. (2009). On the social construction of social problems and social problems theory: A contribution to the legacy of John Kitsuse. *The American Sociologist*, 40(1-2), 61-78.
<https://doi.org/10.1007/s12108-008-9059-5>
- Weinstein, D. (2014). Snowden and U.S. cyber power. *Georgetown Journal of International Affairs*, 4–11. <http://www.jstor.org/stable/43773644>
- West, A., Lewis, J., & Currie, P. (2009). Students’ Facebook “friends”: Public and private spheres. *Journal of Youth Studies*, 12(6), 615–627. <https://doi-org.proxy.bib.uottawa.ca/10.1080/13676260902960752>
- Wing, C., & Steeves, V. (2005). *Young Canadians in a wired world, phase II: Trends and recommendations*. Media Awareness Network.
- Yoo, J. (2014). The legality of the National Security Agency's bulk data surveillance programs. *Harvard Journal of Law and Public Policy*, 37(3), 901-930.
<http://search.proquest.com/docview/1555335569?accountid=14701>