Intermediation and Governance of Digital Flows: Canadian Internet Service Providers as Instruments of Public Policy

by

Michael Zajko

A thesis submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Department of Sociology

University of Alberta

Abstract

The internet has often had a disintermediating effect, 'disrupting' and circumventing traditional middlemen and gatekeepers. This dissertation examines the related trend of intermediation, or the ascendance of new internet intermediaries and their growing significance in our lives. Among these institutions, Internet Service Providers (ISPs) occupy a fundamental position in the internet's topography as operators of material infrastructure, rooted in territories where multiple government agencies exercise regulatory control. As a result, ISPs have become ideal and idealized instruments of governance for the twenty-first century. They are seen as the means through which all of the various dreams associated with connectivity can be achieved. ISPs act as agents of economic and social development, as well as instruments of regulatory capitalism: where 'market forces' fail to produce desired outcomes, ISPs can be steered into desirable conduct through regulatory regimes. As intermediaries become increasingly capable and vital stewards of society's data flows, they are subject to growing expectations on their conduct. Drawing on theories of governmentality and nodal governance, I argue that ISPs are accumulating new roles and responsibilities as sites of governance, but these roles can also contradict one another, resulting in persistent forms of role conflict. These include conflicts over ISPs' roles and responsibilities in aiding policing and surveillance, cyber security, copyright enforcement, and privacy protection. They also involve continuous regulatory struggles about the responsibilities that different classes of ISPs have to one another, efforts to mold the Canadian government's vision of a 'competitive' telecom industry into existence, and the persistent challenge of extending broadband connectivity beyond Canada's urban centers. Drawing on telecom industry/policy presentations, expert interviews, and documents, I show how intermediaries navigate these conflicts individually or collaboratively, choosing a path through competing expectations, serving as policy instruments as well as agents of governance.

Preface

This thesis is an original work by Mike Zajko. The research project, of which this thesis is a part, received research ethics approval from the University of Alberta Research Ethics Board, Project Name: “Internet Intermediaries and the Governance of Digital Flows” (Pro00033715) on September 21, 2012.

Acknowledgements

This research received support from a variety of sources, the most fundamental of which has been my family, who helped me to complete this endeavor through their love and understanding. Staff and faculty at the University of Alberta’s Department of Sociology have also been crucial, principally Dr. Kevin Haggerty, whose willingness to back me wherever my interests led gave me the freedom to explore an inspiring topic, and whose mentorship helped me navigate key junctures and dilemmas. Members of my candidacy and examining committees (especially Dr. Harvey Krahn and Dr. Geoffrey Rockwell) provided valuable feedback, and in what can sometimes feel like a lonely road, fellow graduate students from the department helped sustain me through their collegiality, kindness, and humor.

I thank all of the individuals who contributed their time and expertise to this project, either as interview participants, informal contacts, or discussion partners. Some of these interactions were made possible by the various events and conferences where the people responsible for the internet meet one another. I’m grateful to all those who organize such events to facilitate telecom infrastructure’s social dimensions, and to those professionals who help inform public understanding of their world, which might otherwise be hidden from view.

Finally, I would like to acknowledge the Social Sciences and Humanities Research Council of Canada (SSHRC) for funding this study, in addition to funding from the University of Alberta and its Department of Sociology.

Contents

List of Abbreviations

BRC – Board of Railway Commissioners
CACP – Canadian Association of Chiefs of Police
CATV – cable television (originally Community Antenna Television)
CBCA – Connecting British Columbia Agreement
CCAICE – Canadian Coalition Against Internet Child Exploitation
CCIRC – Canadian Cyber Incident Response Centre
CDN – Content Delivery Network
CNOC – Canadian Network Operators Consortium
CRTC – Canadian Radio-television and Telecommunications Commission
CSE/CSEC – Communications Security Establishment
CSTAC – Canadian Security Telecommunications Advisory Committee
CTC – Canadian Transport Commission
CTCP – Canadian Telecommunications Cyber Protection Working Group
CWTA – Canadian Wireless Telecommunications Association
ICANN – Internet Corporation for Assigned Names and Numbers
ICT – Information and communications technology
IETF – Internet Engineering Task Force
IISP – (In)dependent Service Provider
ISP – Internet Service Provider
ISED – Innovation, Science and Economic Development Canada (formerly Industry Canada)
ITAC – Information Technology Association of Canada
IXP – Internet Exchange Point
NCECC – RCMP National Child Exploitation Coordination Centre
OPC – Office of the Privacy Commissioner of Canada
OSP – Online Service Provider
REN – Research and Education Network

List of Figures

Introduction

The starting point of this dissertation is a simple sociological observation: more and more of our interactions with each other and the world around us occur through an intermediary. These are the hidden parties embedded in the middle of our social relationships, and they do far more than act as messengers or relays. There are two understandings of an intermediary that are relevant here. The first points to whatever (or whomever) sits between the two or more parties involved in a communication. The second definition points to how an intermediary mediates these communications, or how intermediaries govern our digital flows. That is to say, intermediaries should be thought of as "potential points of control" (DeNardis, 2014; Nottingham, 2014; Zittrain, 2003) – a definition based on their ability to affect the communications passing through them. Intermediaries are vital to contemporary society not just because they provide a connective layer for social interaction, but also because they exercise control over how human communication takes place.

The trend towards increasingly powerful intermediaries has been developing over the previous two centuries, as telecommunications networks have come into widespread use and branched across the globe. However, because the intermediaries we depend on seem invisible, we rarely give them much thought. Our communications interfaces are our 'devices'. The world behind the devices, or what connects one device to another, tends to be obscure. The opacity of the world behind our screens, and its growing impact on our daily lives, makes it critically important as a domain of study. We need to understand how this digital world is governed in order to understand how it governs us.

This dissertation expands the topic of internet governance beyond the traditional realm of networks, standards and protocols, to society itself. Rather than discussing governance *of* the internet, I will analyze governance *through* the internet. Specifically, how have the most fundamental digital intermediaries – internet service providers (ISPs) – become instruments and agents of public policy, and to what effect? What political desires can be achieved through these institutions? There is a long and growing list of answers to this question, but I will focus on those that have proven particularly relevant to Canadian telecom politics over the past twenty years.

The period that I am considering has often been associated with neoliberalism, and neoliberal arguments do draw our attention to the primacy of economic justifications for connectivity and telecom policy since the 1990s. However, I argue that neoliberalism is a partial and misleading explanation of contemporary telecom governance in Canada, which is most accurately characterized through the concept of 'regulatory capitalism' (Levi-Faur, 2006). Canadian telecom is now largely the responsibility of competing private firms providing connectivity as a market good. However, the market for connectivity is highly regulated, and ISPs must satisfy an increasing number of public policy obligations. Regulatory capitalism provides a framework for thinking about private actors being used to advance public policy in a regulated market.

While the shift to regulatory capitalism has set the context for internet governance in Canada, another complementary shift has been taking place following liberalization and the commercialization of the internet. Intermediation refers to the growing concentration of power and capacity in the internet's 'middle', where ISPs reside. Typically, such power does not oppose state regulators, but is demonstrated in ISPs' growing capacity to govern society, making them even more attractive and important as instruments of public policy. This seems contrary to the disintermediation often attributed to internet technologies, as these 'disrupt' and circumvent traditional gatekeepers. But alongside this trend of disintermediation, we see the ascendance of new intermediaries and their growing significance in our lives. Google and Facebook are the most visible manifestations of this trend in North America, but ISPs occupy a fundamental position in the internet's topography and are subject to more localized forms of regulatory control. As a result, ISPs have become ideal and idealized instruments of governance for the twenty-first century. They are seen as the means through which all of the various dreams associated with connectivity can be achieved. A neoliberal approach would argue that these dreams are best served by a deregulated market, but under regulatory capitalism, where 'market forces' fail to produce desired outcomes, ISPs can be steered into desirable conduct through regulatory regimes.

As ISPs become increasingly capable and vital stewards of society's data flows, they are subject to growing expectations on their conduct. These expectations overlap and may contradict one another, resulting in persistent forms of role conflict. Intermediaries navigate these conflicts individually or collaboratively, choosing a path through competing expectations. The results often fail to produce the intended public policy outcomes,[1] but the persistence and expansion of intermediary obligations speaks to the growing use of these institutions as instruments for governing society.

I am interested in how the institutions that build telecom infrastructure and allow us to connect at home have increasingly become seen as instruments of public good, guardians of order and morality, enablers of self-determination and economic prosperity, as communal resources, and objects of political struggle. I will consider several of these aspects of

[1] See Walters (2012, pp. 75-76) on the importance of analyzing the relationship between governance and failure to avoid “making governance seem much more coherent and pristine than it really is”.

intermediation through major political conflicts and “problematizations of government” (Dean, 2010, p. 38) that have played out in Canada since the mid-1990s. These include conflicts over ISPs' roles and responsibilities in aiding policing and surveillance, cyber security, and copyright enforcement. They also involve continuous regulatory struggles about the responsibilities that different classes of ISPs have to one another, efforts to mold the Canadian government's vision of a 'competitive' telecom industry into existence, and the persistent challenge of extending broadband connectivity beyond Canada's urban centers.

Outline of the dissertation

After explaining the theoretical and methodological basis for this study (Introduction) and situating the political economy of internet access in a historical context that distinguishes regulatory capitalism from neoliberalism (Chapter 1), the remainder of the dissertation will be devoted to two sets of problems that have significant implications for ISPs in Canada. The first set of public policy debates covered in this dissertation deal with the problem of how to improve connectivity (Chapter 2), and what it means to do so through a commitment to competitive market forces (Chapter 3). The governmental response to this problem has been to mandate that ISPs build and operate certain kinds of networks, and that they relate to one another in particular ways. Because ISPs constitute points of control over the data flowing through their networks, they are also implicated and engaged in a number of public policy debates over how this data should be governed. These include debates over how to manage internet traffic (net neutrality, security), and whether intermediaries should collect and disclose information about digital flows, the activities of users, and their identities (privacy, lawful access). These topics will be addressed in Chapter 4 and 5, which detail how ISPs have become relevant to copyright and law enforcement, national security, traffic management, and privacy protection.

Chapter 2 discusses how extending and deepening connectivity is an important public policy goal in itself, which some intermediaries have been given an explicit obligation to pursue. Access to broadband networks is widely-understood to be 'vital' to society, and this access is valued to enable other ends, such as economic development and education. Since the liberalization of telecom regulation in the 1990s, Canadian public policies to improve connectivity have been shaped by the federal government's commitment to market forces and competition among private networks. In other words, improving connectivity is an important public policy priority in Canada, but the pursuit of this priority must align or contend with a governing rationality that privileges economic considerations and competition between private companies for 'consumers' of services. The result is a role conflict when commercial intermediaries provide connectivity as a public good, and when public intermediaries operate in a predominantly commercial industry.

Canadian ISPs have been called upon to provide greater connectivity, to meet demand with supply, and to do so according to market principles. But 'the market' often fails to deliver what is expected of it, and Chapter 3 addresses the consequences. Relations between ISPs have been regulated with the aim of steering the industry towards greater competitiveness. It was imagined that once the aim of this regulatory regime was achieved, the hand of government would fall away and relationships within the telecom industry would be determined by market forces. However, market forces have not complied with regulatory desires, and incumbents (corporations that held monopolies prior to liberalization in the 1990s) have been able to maintain their dominance in exchange for acting as the instruments of regulated competition. As a result of decisions made by the Canadian Radio-television and Telecommunications

Commission (CRTC), an elaborate regime mandates that dominant ISPs protect the viability of their smaller competitors, restricting incumbents' competitive advantages. In recent years, this regime has become less about forging a new, competitive telecom industry, and more about preserving what competition currently exists from unchecked incumbent power. Instead of facilitating a process of deregulation, this form of regulatory capitalism has become entrenched. The role conflict that inevitably results from this regime is due to the fact that some ISPs are simultaneously expected to compete and cooperate, and that small ISPs are both customers and competitors to the large incumbents that dominate the internet's 'bottleneck' facilities.

The second set of regulatory regimes discussed in this dissertation govern information passing through intermediaries' networks, and the personal information that they hold in their possession. As service providers gain custody over increasing volumes of highly-sensitive information, their importance as privacy custodians has been brought into starker relief and explicitly recognized as a core responsibility. Chapter 4 traces how intermediaries' privacy expectations developed, and argues that some ISPs are adopting a more positive orientation to this responsibility. This means that some ISPs are actively taking steps to advance privacy, rather than treating privacy protection as a set of limitations on conduct. However, commitments to privacy stewardship are often neutralized through contradictory legal obligations (such as mandated surveillance access) and are recurrently threatened by commercial pressures to monetize personal information. Intermediaries exercise considerable discretion in navigating these role conflicts, and some ISPs have sought to distinguish themselves by elevating privacy as a value, while others have chosen to exploit or disclose personal information to meet commercial and surveillance expectations.

Finally, Chapter 5 deals with ISPs' security and surveillance responsibilities, first in struggles over lawful access, and more recently in the domain of cyber security. As with their privacy responsibilities, ISPs have historically exercised significant discretion in governing data towards these ends. However, there have been substantial and repeated efforts by the federal government to standardize ISPs' conduct and expectations, thereby limiting their discretion in matters of security, public safety, and law enforcement. These include repeated versions of lawful access legislation, and cyber security collaboration or 'partnerships' between industry and state agencies. For ISPs, securitization involves a significant role adjustment that moves them even further from the traditional neutrality of the 'mere conduit'. Cyber security programs are a crucial frontier of telecom governance, transforming intermediaries away from the ideal of a ‘dumb pipe’ (that simply carries traffic) and towards intelligent networks that act upon data flows and protect against cyber threats.

My analysis proceeds by identifying some key “problematizations of government” in Canadian internet policy, or “the moments and the situations in which government becomes a problem” (Dean, 2010, p. 38). These are concrete events and cases that call internet governance into question, surfacing tensions around the proper role of intermediaries. Recent years have seen a number of dramatic contests in internet policy, both domestically and internationally, and attending to these problematizations allows us to examine specific practices of internet governance under regulatory capitalism. In Canada, constitutive moments have steered internet politics and public policy down particular directions – including disputes over liberalization, copyright reform, usage-based billing, the public backlash against the lawful access provisions of Bill C-30, and the Snowden revelations. A significant trend seen throughout these topics is a growing public involvement in previously obscure and esoteric issues, elevating telecom policy to the highest level of political visibility.[2]

In the remainder of this introductory chapter, I will define some of the central concepts at the heart of these concerns, including ‘the internet’, as well as different categories of intermediaries and their governing actors. I will explain, through some simplified examples, how the internet functions and is organized, and lay out my theoretical commitments as well as the methodologies employed in my dissertation research.

Defining internet

There are some competing answers to the question of what counts as an internet intermediary, or specifically, an ISP, but I want to begin with the even more fundamental question of what we mean by ‘the internet’. An object so central to this analysis deserves a clear definition, but it is also important to recognize that it is this very definition which is also at stake in the topics discussed herein. In other words, some of the key conflicts over telecom policy can be understand as disagreements over what the internet is, and what it should be (D. P. Reed, 2013). Regulatory distinctions sometimes rest on the contentious matter of what counts as part of the internet, particularly in the debate over the status of new vertically-integrated services (Abma, 2014). Before getting entangled in these matters it is best to start with some agreed-upon basics.

A pedantic definition of the internet would almost certainly include mention of the

[2] For instance, in 2013 some Canadian incumbents and the federal government waged a public relations “war” against each other (Dobby, 2014a), with both sides seeking public support for their respective visions of competition. During the same year, network roaming charges and rural broadband became part of the Prime Minister's Speech from the Throne (Government of Canada, 2013b). The advocacy group OpenMedia.ca has played an important role in mobilizing public sentiment on several issues covered in this dissertation, and formerly esoteric questions of internet governance have increasingly seen significant public engagement. Some individuals have managed to work their own personal complaints through the CRTC's byzantine regulatory process, at times prompting the regulator's judgment on a matter that industry players would rather be left alone (Dobby, 2015a).

TCP/IP protocol suite and internetworking, characterizing the internet as a ‘network of networks’ that stretches across the globe. In short, the internet is the totality of all the digital networks around the world linked through common protocols (principally TCP and IP, but including a number of others). This allows a computer attached to one network to communicate with a computer linked to another, as long as the two networks can connect through the internet.

Network protocols define how information is structured and read by devices connected to the internet. Protocols are not enforced by any one body, but are standards of behavior agreed upon in the interests of common intelligibility. An internet ‘packet’ or ‘datagram’ is transmitted as a series of bits (commonly represented as 1s and 0s). The meaning of each bit in such a series depends on the protocol being used to read it. If a computer assumes that a packet is formatted according to the internet protocol (IP), then the packet’s first 160 bits (the ‘header’) will provide the information the computer needs to handle it properly. For instance, the first four bits will tell the computer which version of the protocol is being used. Another part of the header tells the computer where the packet came from, which is followed immediately by the destination address, so the computer knows where to deliver it (if it is not the intended recipient). This 'metadata' is only meaningful if the parties to a communication have a shared understanding of the protocols involved – that is, they must agree to speak the same language. It is this use of discrete data packets that differentiated the internet’s (packet-switching) architecture from the circuit-switching network design which preceded it (as implemented in traditional telephone networks, see Leiner et al., 2009). This allowed for a decentralized network topography, since packets could simply be handed from one machine to another until they reached their destination.

At this point, our definition of the internet involves computer networks which are connected to one another, and which communicate using shared protocols. Use of the protocols does not make a network part of the internet (the network might be isolated from all others). Instead, the internet refers to the global interconnectivity that its protocols enable. From here, we might pursue a number of different lines of inquiry which would constitute ‘the internet’ as an object of research. Doing so, we might focus on one of the five dimensions of the internet as outlined below. Some of these dimensions will be more relevant to this study than others, but all are part of a holistic definition of the internet.

Figure 1: Dimensions of the Internet: Material to Abstract

Dimension	**Example**
Material	Cables, routers, spectrum
Data	Protocols, packets, information
Institutions	ISPs, registries, regulators
Experience	Online spaces, watching, embedded computing
Myth and Discourse	Metaphor, history, possibility

First, there is a tangible, material dimension of the internet as physical infrastructure. The internet's cables run in thick bundles under the oceans. They pass through conduits under our streets, connecting our home modems to large ‘carrier hotels’ like 151 Front Street in Toronto, which is occupied by floors upon floors of humming hardware. Wireless connectivity is also made possible by material transmitters and receivers, and the physical properties of the electromagnetic spectrum. All of this material infrastructure is owned (or licensed), managed, and regulated. The material dimension of the internet imposes constraints that require governance. For instance, the electromagnetic spectrum has a finite capacity to carry information, and is a carefully managed resource. Installing conduit requires digging up municipal streets, and wires can only be hung on utility poles where space exists. Governing the internet's material dimensions raises questions of private ownership and shared public infrastructure, of the kinds of equipment that ISPs must install and operate, and the legal jurisdiction in which the infrastructure resides (see Goldsmith & Wu, 2006; Melody & Møller, 2001).

Conceptual models of the internet often distinguish ‘layers’ of data running atop a physical base.[3] Rather than committing ourselves to this stratified view of the internet's dimensions, we can consider the physical dimension as a transmission medium for the data circulating through it. This data dimension sees the internet primarily as information, but the information is read by machines rather than humans. Routers send data packets from one link in the chain of intermediaries to the next, and along the way the data can be translated from one transmission medium (Ethernet, fibre-optic, the air) to another. Packets come in many shapes and sizes, and may receive differential treatment by networking equipment.[4] A separate set of internet governance debates deals with how traffic is managed or policed – which forms of discrimination among packets are acceptable, or what forms of content (like spam or child pornography) should be banned and how (see MacKinnon, 2012; Zittrain, 2003).

A third analytic focus for internet studies has been the institutional dimension, encompassing all of the human organizations that structure, coordinate, manage, and shepherd

[3] Typically, explanations of how the internet works distinguish between a number of different layers, beginning with a base, physical layer atop which various protocols and applications rest. However, these explanations differ in terms of the number and nature of layers specified (Galloway, 2004, pp. 39–40; Murray, 2007, pp. 43–46; Zittrain, 2008, pp. 67–69).

[4] For instance, delay-sensitive protocols, such as those used for voice communication, might receive priority over e-mail.

the internet's material dimension and the flows of data it carries. This level of analysis has been particularly important for internet governance scholars, since these are the institutions which govern the first two layers (material and data) and contribute to the production of the other two (experience and myth). Notable internet institutions include the Internet Corporation for Assigned Names and Numbers (ICANN), which administers the “root zone” of the Domain Name System (DNS), thereby constituting a centralized point of control over the whole internet (Mueller, 2004). Another important institution is the Internet Engineering Task Force (IETF), which is an open, collaborative body that develops internet standards and protocols and promotes their adoption by the operators of internet infrastructure (Hoffman, 2012). But ultimately it is up to the networks of the internet, most notably ISPs, to decide whether or not to implement the IETF's standards. ISPs must decide how to manage their traffic and subscribers, and maintain relationships and responsibilities, including those to other intermediaries or to legal authorities. But ISPs have received little scholarly attention as agents and instruments of internet governance, even though it is their decisions, more than that of any other actor, which shapes the experiences of internet users.

These experiences can be thought of as the internet's fourth dimension. Many people have little understanding of the internet's physical layer, the packets carried over it, or the institutions involved in keeping it running. Instead, the internet is the world that exists through the screen: information, social media, and videos. Some users in developing countries know the internet as Facebook, since Facebook is the only application they can freely access (Mirani, 2015). This is the internet as it is experienced and incorporated into everyday life (see Wellman & Haythornthwaite, 2002),[5] in ways that are increasingly pervasive and subtle. We can think of the

[5] A great deal of internet research has employed spatial metaphors such as cyberspace (see M. Graham, 2013),

experienced internet as the product of the first three dimensions.[6] We experience the internet whether or not we understand how connectivity is affected by the physical capacity of networks, the routing of data packets, or the institutional relationships between ISPs and regulators. Studies of internet governance rarely pay close attention to this dimension.

The final dimension or level of analysis could be called the “internet imaginaire” (Flichy, 2007), referring to the ideas we have about the internet, its myths (Mosco, 2004), stories, and dedicated discourses.[7] These discourses and narratives shape how we understand internet technologies, their possibilities and implications. They are produced by the internet's relevant institutions (including its agents of governance), but also through a broader set of processes that include science fiction books and movies, commentators, bureaucrats and academics (M. Graham, 2013). Professionals who operate or govern the internet have been said to share something like a “collective vision” (Flichy, 2007, p. 4). On occasion, we can see how powerful myths and imaginings drive the creation of infrastructure and institutions. Utopian ideas can mobilize participation in network-building as a “great project” (Flichy, 2007, p. 29), such as Australia's National Broadband Network (“At home with the NBN,” 2011). A lack of vision or “compelling narrative” has frequently been identified as an obstacle to new broadband projects (see Wolfe, Vennard, & Mitchell, 2014). However, up to now there have been no studies that show how these narratives, myths, imaginings and discourses lead to the production of certain kinds of networks or determine how they are governed.

analyzed the nature of virtual or online spaces (Turkle, 1994), or studied the interactions that take place in 'discursive space' online (Mitra & Watts, 2002). However, the current trend in internet studies is to critique the idea that online experiences are somehow separate from 'real life', and instead to explore the many ways our reality is digitally-mediated (J. E. Cohen, 2012; M. Graham, 2013; Wellman & Haythornthwaite, 2002).

[6] Experiences and uses also depend on numerous other factors not elaborated here (such as software and design choices, enduser equipment, subjectivity).

[7] Herein I am referring to discourses about the internet, not discourses that exist online or in an internet-enabled discursive space (Mitra & Watts, 2002).

All of these dimensions of ‘the internet’ have been the focus of previous scholarship, and resulted in very different forms of analysis. Since my focus is on internet governance through intermediaries, the most fundamental of which are ISPs (see Goldsmith & Wu, 2006, pp. 70–73), I will necessarily devote much of my analysis to the internet's institutional dimension. The other dimensions of the internet are also relevant for internet governance in various ways, specifically in how material, data and experience are frequently targeted for governance by imposing certain roles and responsibilities on ISPs. Myth and imagining can also be an important factor shaping how the internet is governed, motivating or justifying decisions. But the agents of internet governance are institutions, or individuals working through institutions. These actors decide which networks connects to which, and on what terms, or where the fibre-optic cables run, and who can use them. Institutions determine the ‘user experience’ of the internet in ways that users are often unaware, differentiating and prioritizing some data flows over others. And this is precisely what makes ISPs such important nodes in internet governance – because they are located immediately and directly upstream of users' individual experiences.

Before I turn to discuss ISPs as a particular class of intermediaries and as collective actors, an introduction to internet topology and the ways that different intermediaries relate to one another is required. In this regard, we can consider some of the intermediaries involved in two relatively ubiquitous and straightforward acts – viewing a webpage or playing an online video. In both cases, multiple intermediaries must work in sequence for the act to succeed. At the click of a button, a chain of intermediaries comes into play, translating and transporting information from one internet-connected device to another. If a link in the chain fails, the internet's protocols are usually able to route to a different path. However, not all intermediaries can be circumnavigated, and the internet has evolved into something that is far from the decentralized ideal of its originators. Before discussing the implications of this shift, a simplified, idealized example can help us understand what made the internet so unique to begin with.

The simplified web

In this idealized world, Ada wants to access a website that is hosted on her friend Bab's computer, which sits on the other side of the planet. Between Ada and Bab's computers are several hundred meters of copper and tens of thousands of kilometers of fibre-optic cable. These cables and the equipment joining them together can be broken down into a series of segments, with each segment being part of a distinct ISP's network. Data travelling from one endpoint of the internet to another is passed from one network to the next until it reaches its destination. Some ISPs are known as 'last-mile' providers and serve subscribers (like Ada and Bab) at the endpoints. Other ISPs sit at the 'middle-mile', acting as intermediaries to other intermediaries, or selling wholesale internet to last-mile ISPs.

Information moves both ways along the internet's cables, since in order to access or download content (downstream), Ada must first send 'packets' of data announcing herself (upstream) and then request the content from Bab's server. Ada's request travels from her computer, through her home router and modem, and along the cables that are strung over her street. Her request then moves in and out of neighborhood cabinets and ISP offices. At these locations, Ada's packets are 'aggregated' with those of other users as they are channeled through 'pipes' of increasing size. First her packets join those of other residents in her neighborhood, and then they are combined with the outbound traffic leaving her city along a buried fibre-optic cable.

After they leave her city, Ada's packets are handed from one ISP to another[8] at a location called an internet exchange point (IXP) or 'carrier hotel'.[9] Inside this windowless building, numerous internet pipes, each with a different owner, come up through the basement and meet at a shared 'switch' or a 'meet-me-room'. It is here that the individual networks that make up the internet can physically connect to each other, or plug into each other's equipment. At an IXP, each network 'announces' what destinations can be reached by going through it. In a sense, these buildings are like crossroads, with each road snaking out through the basement and signposted with a list of the many possible destinations along its course. Reaching Bab's address is not as simple as finding her name on one of these road markers, since there are multiple possible routes to any destination on the internet. The best path to take is not simply the shortest, but is defined by the relationships that networks have with one another. Some networks freely accept each other's traffic, but other networks are the equivalent of toll highways – charging for every packet.

Ada's packets are steered out of the IXP, joining one of the large, high-capacity pipes that connect one continent to the next. Along the way, her packets will pass at least one spy agency's listening equipment, which copies them and gives a 'sniff' to see if they are worth holding onto. Once Ada's packets land on Bab's continent, they follow much the same process as above –

[8] There are different kinds of ISPs, and the term is not applied consistently to all of them (the networks that comprise the internet are also organized as Autonomous Systems [ASes]. However, not all ASes are ISPs – some are enterprises, government institutions or CDNs). Some ISPs serve residential or business subscribers, while others serve only other ISPs, or connect government facilities. ISPs can often be organized in a vertical or hierarchical fashion, and if we imagine the internet flowing downward it is possible to distinguish "upstream" ISPs such as the top-level "Tier 1 ISPs" (which typically enjoy massive coverage across the globe), from "downstream", "Tier 2" or "last-mile" ISPs that connect individual users (the term "eyeball network" is also increasingly used, see Faratin et al., 2008, p. 58). ISPs at different levels or positions in the network must form relationships with one another to exchange traffic and access the global internet. ISPs therefore regularly enter into negotiations with each other to decide whether they will impose transit fees, or determine the conditions under which they will exchange traffic as "peers" (see Norton, 2011; Van der Berg, 2008).

[9] For more on IXPs see Weller and Woodcock (2012). Alternately, the interconnection can take place within one of the ISP's facilities.

handed from one network to the next, along smaller and smaller cables, until they are carried across the 'last mile' of telephone-era copper that connects the buildings on Bab's street.

Ada and Bab send each other several packets this way in order to establish a connection, and then Ada receives a stream of packets from Bab which are assembled on her computer's browser as Bab's webpage. The process is experienced as a brief delay between the time Ada clicks on a link and then sees the page on her display. It is a kind of magic. The technology delivers her expectations, with all of the 'how' hidden within wires and locked carrier hotel rooms.

When magic fails

Many of us take the kind of magic described above for granted. The internet is so transparent in its workings, that its presence is often invisible. The only times it rises to our attention is when the magic breaks. During a coffee break at an industry conference,[10] a manager of a small ISP explained to me the frustration of dealing with customers' magical thinking, particularly when the internet's magic does not work as expected. An ISP may not be responsible for the problem, but often becomes the target of customer frustration. Most of us lack a fundamental understanding of how the internet works, even though we have come to rely on it so heavily. Interestingly, people who have come to know the 'how' of the internet can find it incredible in an altogether different way.

In the same coffee break, surrounded by ISP representatives, regulators, vendors, and assorted industry affiliates milling about a hotel conference hall, we began discussing what distinguished people "who know what they are talking about" regarding the internet, from those

[10] The 2014 British Columbia Broadband Conference.

who do not.[11] A network engineer from a major international carrier chimed in to offer his view: those who don't know are amazed at what they can do on the internet, while those who do know are amazed that it works at all. In other words, the technology seems like magic from the outside. On the inside, the magic is that the internet actually works, given how it is put together and governed. The engineer was referring to the informal “handshake” agreements that set the terms for how internet traffic is exchanged between many ISPs (see Weller & Woodcock, 2012). However, he may as well have been talking about any number of other aspects of internet infrastructure and its institutional (and interpersonal) relationships. As scholars, we can come to appreciate this when the internet 'breaks' in particular ways, providing opportunities to study just what holds it together.

The important thing to realize is that simple communications through the internet activate chains of intermediaries who must work in concert. These chains can include multiple ISPs handing traffic to one another, IXPs and the organizations that host them, popular online service providers (OSPs) like social media and video streaming sites, as well as the content delivery networks (CDNs) that OSPs depend on to keep their data distributed. Any link in this chain could become congested with traffic, either through high demand or due to a malicious denial-of-service attack. Any two intermediaries in the chain might have a dispute, with one party refusing to serve the other. Traffic sniffers (or deep packet inspection [DPI] equipment), like those employed by intelligence agencies, are also used by ISPs to identify the sorts of traffic carried across the network, where they can be used to block undesirable packets.

Each link in the chain between intermediaries can be a chokepoint, or a point of control. The internet's foundational myth is that it was designed to survive a nuclear attack, and can

[11] Since earlier in the conference, a provincial government minister had mixed up megabits and megabytes in his presentation.

automatically reroute around problems such as those listed above. But there is only a small element of truth to this story (see Hafner & Lyon, 1996), which might best be described as the “false rumor” of the internet's origin (Leiner et al., 2009, p. 776). Certainly, the packet-switching technology underlying the internet allows for a high degree of resilience, but this depends on the topography of the networks involved in a communication. This topography has changed immensely since the early days of the internet.

The changing internet

The internet is still a branching, decentralized network-of-networks, but its core is composed of enormous entities that handle the majority of communications among themselves. In other words, the internet's topography has been flattening in recent years (Sandvine, 2013, p. 6), as some large intermediaries have come to occupy a greater number of roles. Where previously, several links in the chain of internet intermediaries could be organized hierarchically, now most traffic circulates between a small number of players, some of whom have grown into expansive “hyper giants” (Labovitz, Iekel-Johnson, McPherson, Oberheide, & Jahanian, 2010, p. 4). Google is one of the best examples of this trend, if we consider how the company has steadily accumulated new roles and assets over its history. Google could be considered an OSP (providing a large number of online services), or a CDN. It maintains an extensive worldwide fibre-optic backbone and even serves as a residential ISP in select US cities. While its Google Fiber residential service remains a limited project, the company's online services (like YouTube) are typically accessible through a direct connection to any of North America's major ISPs. The majority of North American traffic now flows through direct, private connections, between vast incumbent ISPs with millions of customers (Bell, Rogers, Shaw, TELUS) and the servers of content giants like Google.

This flatter, disintermediated internet has been likened to the “walled garden” networks pursued by early private internet providers such as AOL (Paterson, 2012). While even vertically-integrated incumbent ISPs do not contain their subscribers within closed networks (although they move closer in this direction when they offer their own streaming video services, see Dobby, 2015b), the trend is certainly that of more traffic exchanged between fewer and larger players (Labovitz et al., 2010). Those networks at the margins, such as local ISPs, are often highly reliant on their connection with an upstream incumbent. For subscribers of these networks, basic internet connectivity can depend on the crucial connection between the first two intermediaries in the chain.

In addition to the flattening topography of the internet, the roles that intermediaries play have also undergone important changes over the years. As mentioned, intermediaries such as ISPs now occupy a greater number of roles. Part of this has meant that ISPs take more of an active interest in the nature of the traffic in their networks, and make a greater number of interventions. ISPs have come to employ a growing number of “middleboxes”, or intermediary devices (which can be virtual or physical) that have some additional function besides routing traffic (Carpenter & Brim, 2002). Some of the uses of these middleboxes, including packet inspection and traffic interventions, are the same mechanisms employed for computer attacks (Hildebrand, 2014),[12] even though they may be employed by ISPs to detect and block 'malicious' traffic. As another example, Bell has asserted its right to expand into the role of advertiser, by collecting a broad sweep of information about its mobile users and to use this information to serve targeted ads (Henderson, 2014a).

[12] They may also limit individuals' abilities to protect themselves for attack, for example by limiting the use of encryption protocols (Hildebrand, 2014).

As an example of how middlebox functions can break internet communications, we can consider the previous example of Ada connecting to Bab's webpage. The scenario was based upon some idealized assumptions about the internet, and in reality Bab would very likely find that her ISP has made hosting a web site from home an impossibility. This could be because her ISP's middleboxes block certain kinds of traffic, or because of the ISP's use of Network Address Translation (NAT), so that she does not have a stable, unique IP address that can be used to locate her server. These interventions are not necessarily designed to have a gatekeeping function,[13] but they have a gatekeeping effect. They are also shaped by the expectations that ISPs have of their users. Increasingly, the expectation is that customers can be equated with “eyeballs”, and that residential ISPs have become “eyeball networks” (see Faratin et al., 2008, p. 58). In other words, subscribers are viewers, much as in the days of television, except with more control over how they consume 'content'. This view of internet users neglects their productive capacities, and leads to limits on the possibilities for new kinds of services (since these are envisioned as sending traffic from central servers downstream to the eyeballs or end-users, rather than generated by the end-points of the network). But even eyeball networks can break when they are used for their predominant demand – streaming video.

In an alternate example, we can consider how Ada might watch a video online from the NettyFilms service that she subscribes to. To do so, Ada needs a high-speed connection to NettyFilms' server, which is a computer located in a secure, windowless room deep within the same building that hosts a carrier hotel or IXP. To connect to this room, Ada's request must leave

[13] NAT is, among other things, a way for multiple subscribers to share the same IP address. This is valued by ISPs which have a smaller number of (IPv4) IP addresses than customers, or which have yet to transition to IPv6. However, the widespread use of NAT effectively destroyed the assumption that every device connected to the internet has a unique IP address. As a result, many uses of the network become much more difficult or impossible (Ferro, 2011).

her house through a modem provided by her ISP, and then through the co-axial copper network that this ISP uses to connect its customers to the internet backbone. But Ada's ISP, a smaller provider that we will call IndieNet, does not own the copper network that it uses to send data in and out of Ada's home. Instead, IndieNet leases network access from a larger ISP and cable company, BiggieNet, that owns the copper. IndieNet and BiggieNet must work together to ensure Ada receives smooth service, but their interests do not necessarily align. BiggieNet might be tempted to see IndieNet as a competitor, and place less of a value on ensuring IndieNet subscribers receive good service. BiggieNet might also find itself in a dispute with NettyFilms about which party should be paying the other for the vast amounts of traffic being carried from NettyFilms' servers. Such disputes have led to degraded performance of Netflix in the US (Malik & Higginbotham, 2013), and in Canada, smaller ISPs have complained about unfair treatment by the incumbents they rely upon for service (Freeman, 2013; Kyonka, 2013a).

Now that we have some idea of how the internet works, its multiple dimensions, and how intermediaries fit together, we can turn to a deeper consideration of the most important class of actor in internet governance – those who operate the world's networks and provide access to the internet.

ISPs as instruments of governance

An ISP often functions as a faithful relay, passing packets from one end of its network to another. But in theory these institutions are ideally positioned to inspect and control the entirety of our online communications. They occupy the “pinch points” (Murray, 2007, p. 74) or “points of control” (Zittrain, 2003) where regulatory policies can be imposed for maximum effect. Since ISPs operate gateways to the rest of the internet, they can be enlisted as gatekeepers. If certain kinds of traffic need to be blocked or monitored, this can be done by enlisting the ISP, whether its subscribers are the source or the destination of the traffic (Zittrain, 2003). If an individual internet user needs to be identified, an ISP is in a position to link these online activities with a physical location and a subscriber's account. If the lack of internet access is a concern, then ISPs can be mandated to open their gates wider, build more infrastructure, or offer certain services at a set rate. All of this has made ISPs attractive as instruments of public policy, particularly since exercising internet controls by other means (such as through its “multistakeholder” governing bodies or directly over users' computers) is so difficult. Rather than dealing with the jurisdictional headaches of internet governance, trying to bring distant actors in line with domestic policies, or bringing the internet under direct government control (for instance, through nationalization), governments can use ISPs to achieve their domestic dreams of internet governance.

In general, the roles and responsibilities of ISPs have steadily expanded over time. Their core business remains that of moving data packets between end-users and the rest of the internet, but ISPs now provide a growing number of services to their subscribers, members, or users,[14] and are becoming implicated in a growing number of social concerns. Much of the internet's early success has been attributed to legal limitations on ISP responsibility, which meant that ISPs were not liable for the conduct of their users, as long as they played a limited intermediary role (see Chander, 2013). ISPs are moving further and further away from the ideal of a pure intermediary, or simply a pipe that moves data packets from one edge of the network to the other. As they occupy a more central role as enablers of our daily lives, they have taken on more of the

[14] The terminology varies with the nature of the intermediary. For instance, some FreeNets have 'members', some of whom receive free or subsidized service. An educational network provides connectivity to students, but these are best thought of as users. The term 'user' is perhaps the broadest of all, since it does not denote any sort of business relations (an ISP can carry the traffic of users who are actually the customers of another ISP).

responsibilities that go along with this position – sometimes willingly, and sometimes as an imposition. My focus going forward will be on the instrumental use of ISPs to advance certain forms of public policy, as well as the agency that ISPs exercise in regard to these public policies.

Theoretical background

Empirical research requires a metatheory to provide a basic epistemological and ontological orientation, or some starting assumptions about the world and our knowledge of it. My approach in this regard is aligned with scholars of "critical realism" (Porpora, 2016; A. Sayer, 2000),[15] to the extent that I assume an observer-independent reality exists – a world that consists of real objects, entities, structures, mechanisms, and conditions which are amenable to study, or which we can come to understand through various methods. Critical realism is partly informed (or qualified) by postmodern and constructivist critiques, and is sympathetic towards them, but does not embrace constructivism at a level so fundamental it challenges our ability to understand, analyze, and describe our social reality. While discourse plays an important role in this dissertation, particularly in how it structures public policy and guides government decisions, there is a (largely) non-discursive reality of networking infrastructure to which public policies and regulatory classifications apply.

Whereas my metatheoretical approach can be characterized as critical realism, my interest in intermediaries as agents and instruments of public policy draws on the broad field of governmentality studies, inspired by the work of Michel Foucault. This dissertation is an account of a particular "milieu", as defined by Foucault in a lecture series that would eventually contribute the notion of governmentality. A milieu is "the medium of an action and the element

[15] Critical realism is most fundamentally associated with the philosopher of science Roy Bhaskar, but Sayer (2000) and Porpora (2016) provide practical interpretations for sociologists.

in which it circulates" (Foucault, 2007, p. 21). This also makes the milieu a target of intervention, for what Foucault would describe as techniques of governmentality. In his governmentality lectures, Foucault was primarily concerned with interventions directed at the population, as well as the circulation of goods, people, and of diseases in emerging towns and cities. The relevant milieu for this dissertation is the medium through which data packets circulate, and the interventions that target these flows and their conduits. As information flows and digital identifiers become increasingly consequential, so does control over them. Intermediaries become privileged sites of governance and recurring targets of intervention.

Studies of governmentality constitute a growing field, but these have proliferated along some diverse lines.[16] Foucault did not produce a theory of governance[17] as much as a set of conceptual tools and approaches we can take towards an "analytics of government" (Dean, 2010, p. 30; Walters, 2012, p. 40). In answering the question of how we govern and are governed, Dean distinguishes four dimensions of analysis, including forms of visibility (how things are made visible), ways of thinking and producing truth, ways of forming subjects, and "specific ways of acting, intervening and directing, made up of particular types of practical rationality" (Dean, 2010, p. 33). It is this last dimension that will be the primary focus of my analysis, which will attend to different kinds of rationality that have been applied to the problem of how to govern the internet – including its structure, deployment, and the conduct of its users.[18] Visibility and

[16] This diversity is partly due to the distinct ways in which Foucault himself used the term (see Foucault, 2007, pp. 108-109; Walters, 2012).

[17] Defined as the "conduct of conduct", which Dean has expanded to mean "any more or less calculated and rational activity, undertaken by a multiplicity of authorities and agencies, employing a variety of techniques and forms of knowledge, that seeks to shape conduct by working through the desires, aspirations, interests and beliefs of various actors, for definite but shifting ends and with a diverse set of relatively unpredictable consequences, effects and outcomes" (2010, pp. 17-18).

[18] There are numerous parallels here with Foucault's analysis of "security" as the management of "circulation" in towns and cities of the 18th century by early urban planners (Foucault, 2007, p. 20). The mechanisms of security that Foucault analyzed were developed to deal with the "problem of circulation", or how to control movement,

knowledge production are also important and intertwined with these concerns. For instance, internet surveillance involves making things (and users) visible, as well as producing authoritative knowledge. Telecom regulators collect information about the disposition of the country's networks, and produce an authoritative discourse to which intermediaries are subjected – obliging intermediaries to conduct themselves in ways that comport with regulatory distinctions. I am less interested in how the subjects of internet governance are formed, but this is a question that deserves at least preliminary consideration. In other words, we should begin by considering the nature of the actors who are involved in internet governance.

Foucauldian analyses sometimes present governance as an anonymous landscape of processes, technologies, discourses, strategies and identities. Alternately, they problematize actors themselves, showing how subjects (including individuals and collectives) are constituted (Walters, 2012, pp. 137–138). This is consistent with Foucault's own analyses of how “the subject” is produced, and his rejection of the Enlightenment's rationalist model of the self (Caldwell, 2007; Foucault, 1982). But such approaches paint a picture of reality that not only contradicts common distinctions and forms of sense-making, but can also result in severe ontological limitations for the analyst, including the danger of lapsing into determinism (Archer, 2000).

In general, studies of governmentality make minimal or unstated assumptions about ontology – declining to specify what sorts of actors and forces exist in the world. Instead, governmentality focuses on “regimes of truth, the practices and strategies that ontologize the world in the first place” (Walters, 2012, p. 57; see Foucault, 2007, p. 79). Dean argues that this sort of problematization means doing without any sort of global political theory, and he

exchange, and distribution (2007, p. 64). As these urban planners shaped the flows of people, animals, and goods, agents of internet governance shape today's digital flows and the infrastructure that carries them.

encourages us to examine "the different and particular contexts in which governing is called into question, in which actors and agents of all sorts must pose the question of how to govern" (Dean, 2010, p. 38). And yet, this very statement assumes the existence of "actors and agents" – even if they come in "all sorts". These are actors who can behave in various ways, even as government seeks to shape their freedom (Dean, 2010, p. 21). An implicit or explicit theory of the actor is therefore at work in many contemporary studies of governmentality, and is not without basis in Foucault's own writing.

While on the one hand, Foucault seems to attack the very notion of intentional agency in much of his work (treating agency as an effect of discourse or power), he also makes space for resistance and "acting otherwise" (Bevir, 1999; Caldwell, 2007). This includes the fundamental role Foucault grants freedom and "free subjects" in a late essay entitled *The Subject and Power*, where he argues that "individual or collective subjects... are faced with a field of possibilities in which several ways of behaving, several reactions and diverse comportments, may be realized" (Foucault, 1982, p. 790). On this basis, some authors have attempted to recover workable forms of agency and intentionality through Foucault, and argued that Foucault himself was moving in this direction in his later work (Archer, 2000, pp. 32–34; Caldwell, 2007). Others have built bridges between Foucauldian theory and critical realism (O'Mahoney, 2012) or actor-network theory (Walters, 2012, p. 98; Wood & Shearing, 2007) in order to conceptualize actors and agency in a way that is more productive for analysis.

In light of these arguments and Foucault's own (1982) statements, I will begin with the assumption that actors exist, and that there are useful ways of retaining insights about governmentality while still attributing agency. But this raises the question of what constitutes an actor? Embodiment and consciousness have frequently been the focus of answers to this question

(Archer, 2000; Caldwell, 2007), but I want to examine the possibility of collective agency, and make an argument for why an institution such as an ISP should be considered as an actor.

Individual and collective actors

The chapters that follow are built around arguments and analyses at the level of institutions. I will primarily be interested in relationships between institutions, and the sorts of possibilities that are open to intermediaries, both as instruments and as actors. When I say that an intermediary can be an instrument of public policy, I mean that the intermediary is somehow brought in line, compelled, convinced or enrolled, to act in a way that serves public policy. There are a number of ways of going about this process, which can often be characterized as a form of "responsibilization" (Zajko, 2016a). But I also maintain that it is not sufficient to think of intermediaries as passive objects of policy. Instead, we can think of intermediaries as actors, which, even if they are acting as instruments, demonstrate varying degrees of autonomy, resistance, and discretion. It is this claim which deserves some further explanation, since it may not be self-evident that a group of people tied to a common institution and telecom infrastructure somehow collectively constitute an actor.

In arguing that an intermediary is an actor, or that an ISP can play different roles in society, I am raising the question of what it means to personify or individualize an institution. In everyday speech, collective actors are a sort of shorthand. To say that a private company or a government 'did' something might refer to a decision made by senior executives, some collective 'groupthink', or the result of institutional policies. While we frequently speak and think of institutions such as states and corporations as 'natural' collective actors, it is important to note that these conceptualizations are a "social invention", engendered by larger theories of society as well as legal classifications (Pedersen & Dobbin, 1997). The fact that an organization (which might have several, or several thousand employees) is described as an actor in common speech or a regulatory document may say more about these discursive conventions than the degree of collective agency being exercised. However, even as a kind of shorthand or convention, the notion of collective actors does indicate that we are dealing with institutionalized forms of decision making, and institutions for which identifiable positions are declared.

Analyses of internet governance that engage with social theory have typically avoided deeper questions of collective agency. For instance, Mueller (2010) draws on social theory to elaborate different conceptualizations of networks,[19] and how actors relate to one another, but the fundamental basis of agency is left unexamined. While Mueller sees no need to define what counts as an actor, he does ascribe agency to collectives and institutions. The main distinctions in his analysis are between "state", "non-state", "private" and "civil society actors", all of whom participate in networks involved in internet governance. In other words, organizations that make (or produce) decisions can be treated as actors. Beyond distinguishing different kinds of organizations that might act in distinct ways, Mueller does not feel it is necessary to further problematize the notion of agency.

Scholars of nodal governance, sometimes drawing on a combination of Foucault and Latour, focus on "nodes" as institutional "sites" of governance, or "institutional settings that bring together and harness was of thinking and acting" (Wood & Shearing, 2007, p. 149). In other words, "a node is a point in time and space where a cluster of actors collaborate to mobilize

[19] Mueller conceptualizes networks as modes of organization and methods of association. One kind of a network is than of an organization structured in a network form (albeit with clear boundaries, and perhaps even minimal elements of hierarchy). A looser form of network is that of an "associative cluster" within which actors interact and form relationships, producing "governance as a byproduct of many unilateral and bilateral decisions" (Mueller, 2010, p. 42). In other words, organizations can be structured as networks, but many networks are better considered as forms (or "clusters") of association between actors.

pooled resources" (Braithwaite, 2004, p. 300). These nodes can be "both objects of governance" (which can be enrolled or mobilized by others), "and actors that govern directly or through others" (Wood & Shearing, 2007, p. 27). While the conception of a node as both an object and agent of governance is crucial for my analysis, exactly what counts as a node is left ill-defined in the nodal governance literature. Nodes, "may comprise individuals, groups (and parts of groups), organizations (and parts of organizations) or states—may be large or small, tightly or loosely connected and inclusive or exclusive in membership" (Shearing & Johnston, 2010, p. 501). They are sites a where actors collaborate and pool resources, but can also apparently be analyzed as collective actors.

In general (and as with a lot of governmentality literature), nodal governance scholars are less interested in identifying actors and discussing agency, and more concerned with analyzing "mentalities" and strategies of governance, or discussing networks of power. Sociologists dealing with institutions and organizations have recurrently grappled with the question of collective agency, but this has often been subsumed by the debate over agency and structure – with agency taken to be a property of the individual and structure manifesting as the institution or social system (Domingues, 1995; W. R. Scott, 2004). When the chief distinction is between agency and structure, it become difficult to conceptualize a collective actor that can *also* be a social structure. Scholars who have attempted a more integrated understanding of social dynamics that avoids the reductive poles of agency and structure (with Giddens being the most influential),[20] have typically been less interested in exploring different levels of agency or the foundations of

[20] Giddens' structuration theory addresses the interrelation between individual human agency and structure, arguing that the two are inseparable and mutually constitute social systems. Giddens (1984) includes some discussion of collective action, but makes a distinction between action and agency, attributing the latter to knowledgeable human beings, stating that "only individuals, beings which have a corporeal existence, are agents...[not] collectivities or groups" (p. 220).

collective decision-making.

The simplest solution to the problem of collective agency is to acknowledge agency at the collective or institutional level, but then to ground one's analysis in the least-problematic kind of actor – the individual human. For instance, Castells' (2009) theory of networked power asserts that actors can be individual or collective, but that ultimately “all organizations, institutions, and networks express the action of human actors” (2009, p. 10). Castells takes some steps to link social theory and neuroscience to reflect the primacy of the human mind (2009, Chapter 3), and draws on Giddens' (1984) structuration theory for the link between actors and institutions (Castells, 2009, p. 14), but ultimately provides little in the way of a coherent social theory besides his general statements about how networks and power relate.

Little (2013, 2014) has recently argued that social theorists should not be required to specify the link between collective action and its “microfoundation” in individual actors.[21] The important thing is to “be confident” that this “micro-to-macro” link exists (that there are mechanisms through which individual action contributes to some larger phenomena, such as the behaviour of an organization), and to be able to “gesture plausibly” towards such mechanisms (Little, 2013).[22] Adopting this argument, it seems obvious that a large corporation (or a diverse organization such as an industry association) comprises numerous people helping make decisions, such as what position to take on government policy.[23] But it is not necessary to map the process through which a decision was arrived at if we are more interested in a “horizontal”

[21] A type of explanation called “singularism” (Gilbert, 2014) or “methodological individualism” (Giddens, 1984, pp. 213-214).

[22] Little (2013) also argues that we need “better theories of the actor”, but in the meantime, we do not need to begin with a complete theory of micro-level (individual human) agency in order to arrive at some understanding of social dynamics at the level of larger phenomena, such as institutions (Little, 2014).

[23] As described by one company executive, ISPs “are of course complex organizations whose consistency from one thing to another is therefore not always obvious. They’re themselves the site of pretty convoluted struggles as to what ought to be done” (B. Abramson, personal communication, August 30, 2016).

explanation of how institutions relate to one another, rather than a "vertical" explanation of how a collective decision ultimately rests on a microfoundation of individual human actors (Little, 2013). For such purposes, it seems reasonable to attribute agency to the organization (Little, 2014), even if we understand that individual human agency contributes to the decision-making process.

We can elaborate this position slightly further by drawing on the work of some international relations scholars, who have had to confront similar questions when accounting for the agency and decisions of states and international organizations (see Wendt, 2004). International relations scholarship has also made productive use of role theory to conceptualize corporate or collective actors[24] (see Barnett, 1993; Harnisch, 2011; Thies & Breuning, 2012). Paraphrasing Barnett (1993, pp. 274–276), I argue that intermediaries, as institutions, demonstrate continuity and stability. They can maintain particular positions or patterns of behaviour even as their human constituents change, acting in ways that are not *wholly* determined by (or reducible to) individualized human desires and practices.[25] The organization provides a framework for individual action and a structure for collective decision-making processes. Individuals within an organization are subject to policies, rules and regulations. They may make decisions based on what they think is best for the organization. From the perspective of symbolic interactionism or role theory, individuals can be socialized to identify with the organization (Barnett, 1993, p. 274). In more Foucauldian terms, we could say that the members of an organization are constituted as particular kinds of subjects, and that individuals in an

[24] Corporate actors can be distinguished from collective actors as having some centralized authority and decision-making structure, but whether decentralized or hierarchical, both can be considered under a broader heading of collective agency (Wendt, 2004, pp. 297–298). For more on the various ways of defining and operationalizing corporate actors, see Flam (1990).

[25] For more on this sort of reductionism, in which the actions of a group are said to be reducible to the qualities and interactions its individual members, see Wendt (2004, pp. 298–300).

institution are implicated in regimes of governance at the level of their daily practices (see Walters, 2012, p. 64). An organization (or set of organizations) can be analyzed as a "regime of practices", which "possess a logic that is irreducible to the explicit intentions of any one actor but yet evinces an orientation toward a particular matrix of ends and purposes" (Dean, 2010, p. 32). Either way, it is not sufficient to say that the behavior of organizations can be derived from that of its members. An organization and its human members are mutually constitutive (see Wendt, 2004, p. 307), rather than one being the product of the other.

Intermediaries occupy social roles that cannot be reduced to their human employees, managers, or executives. The roles of intermediaries in society (as economic facilitators, public utilities, surveillance agents, privacy custodians, marketers, and mandated wholesalers) shape their conduct and impose responsibilities. Canadian courts have had to confront this issue directly, where legal responsibilities (specifically concerning copyright) have been deemed to depend on the role (or "function") that an intermediary is playing (*SOCAN v. CAIP*, 2004). Some roles are self-professed and chosen, such as when an ISP chooses to address economic inequality and work towards more equitable connectivity (Monsebraaten, 2013). Other times, an ISP will act in a role mandated by law, such as that of privacy custodian or a wholesale provider, but may choose to do so in a way that exceeds the organization's legal responsibilities. This dissertation does not just concern the pursuit of public policy through the exercise of power over intermediaries, but considers intermediaries both as instruments and agents of public policy.

Since an organization can occupy multiple roles, 'role conflict'[26] results when an

[26] The idea of role conflicts (derived from role theory) has a long history in sociology, where it has primarily been used to analyze how individuals deal with the contradictory expectations attached to some position in a social relationship (Biddle, 1986; Stryker, 1980, p. 73). In the 1970s, role theory was imported into the disciplines of foreign policy analysis and subsequently, international relations, where it has been used to analyze the contradictory roles and expectations of states, organizations, and other institutional, collective or "corporate"

intermediary is subject to contradictory expectations (such as when an incumbent ISP is expected to compete with companies that are also its customers, see Chapter 3). When this happens, one role might become predominant, elevating some responsibilities at the expense of others. As I will show, different intermediaries facing similar role conflicts have chosen different paths, demonstrating the discretion with which organizations can choose to resolve these contradictions.

While intermediaries such as ISPs should be thought of as collective actors, the kinds of organizations considered in this dissertation assume a wide range of forms and sizes. A small ISP, for example, may be one in which all significant decisions are made by one person. A large corporation might operate as a hierarchy, but have managers making decisions at various levels of the organization, often in collaboration with others. A FreeNet might decide by holding a vote of its members, so that the organization's decision is directly shaped by these individual opinions. To say that these are all collective actors is not to say that they are all alike, but that these are all organizations to which we can attribute agency. My conception of collective actors is a “thin” one based on their intentionality, as purposive or goal-directed systems, without making claims about the existence of a collective consciousness or identity (see Wendt, 2004). This is to say, we should accept that collective actors have collective intentions, which are not reducible to the intentions of their individual members. Organizations act in ways that are intended to bring about particular goals, and while these goals may be determined by individuals within the organization, they also have the effect of shaping the behaviour of individuals within the organization to further collective intentions.

actors (Harnisch, 2011; Thies & Breuning, 2012).

Looking across institutions

The analysis I am providing is therefore a “horizontal” one (Little, 2013), examining social relations on the level of institutions. But it is important to keep in mind the vertical dimensions that I am neglecting as a consequence of focusing on institution-to-institution relations. The first is the nature of the social relationship between all of us (as users, subscribers, consumers) and these institutions. This is the dimension which implicates Ada and Bab in the example provided earlier in the chapter. It encompasses how we experience the internet, and how this experience is mediated. It also encompasses how individuals and populations are governed through the internet, such as when individuals are held accountable for child pornography, cyber security threats, or copyright infringement. While the user-intermediary relationship is not the focus of this analysis, it should be clear that this is precisely what is at stake in the forms of governance decided by institutional interactions and relationships.

The other vertical dimension is largely missing from the institutional level of analysis is that of individuals and their contributions to institutional dynamics. I am not providing an analysis of how decisions are made within various organizations, or tracing the roles of individuals in carrying out corporate policies. This is not to say that individuals do not matter, since institutional relationships are mediated through human interactions. Some individuals have a disproportionate impact on the dynamics of the Canadian telecom industry, either through their role in an organization, or through their personal involvement.[27] In many ways, the Canadian telecom industry is a 'small world' built on interpersonal relationships. Telecom industry professionals often hold jobs with several institutions over their careers. It is typical for senior

[27] In recent years the strongest example of an unaffiliated individual participating in Canadian telecom governance has been Jean-François Mezei, who became well-known as a regular attendee at industry events and outspoken participant in CRTC proceedings (Chase & Marlow, 2011).

executives at more recently-established companies to have spent their earlier careers working for the local incumbent. As individuals move from company to company, they accumulate knowledge and personal contacts. The small world of Canadian telecom also fosters interpersonal relations through industry events, where individuals enjoy drinks and meals alongside both rivals and partners. Even among parties with strong disagreements, cooperation on some issues eventually becomes necessary.

Ultimately, internet governance is built on human relationships and has human implications. But the sorts of decisions made about internet governance cannot simply be reduced to the human level. This means considering the role of collective actors and collective decision-making; of institutions that are not just sites of human action but also actors in their own right. These are actors in pursuit of goals and intentions, maintaining corporate positions or changing them as circumstances dictate.

Method

My analysis distinguishes different kinds of institutions and their roles and responsibilities in internet governance. This can be understood as a form of "explanatory mapping" – or the first part of a methodological approach advocated by nodal governance scholars.[28] Paraphrasing Wood (2006, pp. 230–231), such mapping is carried out by answering the following questions:

[28] For Wood and other nodal governance scholars, this descriptive and explanatory process is the first step in a normative project that seeks to design, implement and diffuse "innovations" in governance (Wood, 2006), opening "new opportunities for realizing democratic values" (Wood & Shearing, 2007, p. 115). I consider this normative dimension to be separate from nodal governance as an empirical analytic project and see no reason to advance its particular commitments, although I will discuss the implications of my research to the question of intermediation (versus disintermediation) in the Conclusion.

- Who are the actors involved in governance?

- What forms of knowledge, and what capabilities and resources, does each of these actors bring to bear in governing?

- What does this set of knowledge, capabilities and resources reveal about the world-view, or rationality of such actors?

- What are their stated outcomes and how to they measure success?

- How do these different actors relate to one another? In what situations? With what results?

These questions can be addressed through a mix of methodologies, 'mapping' the nodes and networks involved in governance. In this orientation, “nodes are sites of knowledge, capacity and resources that function as governance auspices or providers” (Wood & Shearing, 2007, p. 27). The relations between nodes are key in this analysis, as governance becomes “the property of shifting alliances” (Johnston & Shearing, 2003, p. 148) and nodes “attempt to mobilize and resist one another” (Wood & Shearing, 2007, p. 149).

Importantly, nodal governance was not developed as an approach for analyzing how digital networks are governed, and so the nodes and networks these scholars refer to are principally social institutions and their relationships, rather than the material infrastructure of digital networks. Furthermore, the argument that governance should be defined as “the property of networks rather than as the product of any single center of action” (Johnston & Shearing, 2003, p. 148), has to be understood as an argument for de-centering state actors, rather than a claim that contemporary governance operates through decentralized networks. For all their talk of nodes and networks, nodal governance scholars sometimes emphasize the importance of hierarchical power relationships.[29] They are also ambivalent about the very existence of

[29] For example, Wood and Shearing argue that “the world of nodal governance is hierarchically structured” (2007, p. 149), although this world consists of multiple overlapping and shifting hierarchies of “weak” and “strong”

networks, which is treated as "a matter for empirical enquiry" (Shearing & Johnston, 2010, p. 500). Hence, these scholars place theoretical emphasis on nodes, with their participation in networks left as an open question. This leads to the methodological principle "that the empirical study of networks should be predicated upon a prior analysis and understanding ('mapping') of the nodes that (sometimes) constitute networks" (Shearing & Johnston, 2010, p. 500).

My own analysis focuses on digital networks and their governing nodes, and I make no presumption that we can learn about intermediaries as institutions of governance by understanding the properties of networks.[30] By steering clear of the generalizations about networks that have become so commonplace in social theory, my focus will remain on the specificity of governance in Canadian telecom, analyzing the relationships between nodes (such as ISPs and state agencies) through empirical inquiry.

Empirical sources and methods

The first stage of my research involved surveying the history and political economy of Canadian telecom through written sources, while attending industry events to get a sense of contemporary issues and relationships. Initially (around 2012), I was interested in public policy debates around lawful access and copyright, as the expansion of ISP responsibilities in these areas had recently been in much dispute. It was only once I started to attend industry events, read industry publications, follow regulatory proceedings, and speak with individuals involved in Canadian telecom that I came to appreciate more mundane pressures and role conflicts. These

actors (Wood & Shearing, 2007, p. 153).

[30] While I, following Latour, oppose a fundamental distinction between "social" and "technological" networks, equivalences between digital communication networks and networks of governance can be dangerously misleading, and so it makes little sense to base an understanding of internet governance on network theory (Mueller, 2010, pp. 17–18).

included the constant tensions between incumbents and their smaller competitors, the coexistence of intermediaries with very different governing rationalities within a single 'market', and the issues around providing connectivity as a public good.

I attended one regional,[31] and four national industry conferences,[32] two major international industry and policy events,[33] and several more specialized meetings dealing with various aspects of internet policy.[34] Presentations and discussions at these events allowed me to identify salient themes and debates in Canadian internet policy, including the dominant concerns within the telecom industry between 2010 and 2016.[35] Often, the most valuable interactions that I observed and participated in took place informally and spontaneously, when a mix of individuals found themselves sharing the same breakfast, lunch, or dinner table. Conversation would turn to some issue of shared concern, and statements were often less-guarded than in conference presentations. I also learned a great deal from numerous individuals with whom I had informal one-on-one conversations. Through these observations and interactions, I was able to identify common themes around which to organize my analysis.

Based on the themes that arose from my initial mapping, I organized the topics of this dissertation into two parts. The first part (Chapters 2-3) addresses the question of what connectivity means and how best to provide it. The second part of this dissertation (Chapters 4-5)

[31] The British Columbia Broadband Conference in 2014.

[32] The ISP Summit in 2012, 2013, and 2014, and the Telecom Summit in 2014.

[33] IETF 88 and NANOG 59, both in 2013.

[34] These included the 2014 IXP Symposium, the 2014 Canadian Internet Forum, ARIN on the Road in 2013, the CPI Citizen Planning Circle on Effective Use of Rural Broadband in Olds in 2014, and the Digital Futures Symposium in 2013, 2015, and 2017.

[35] This involved noting the topics of discussion at Canadian telecom events, allowing me to see which concerns have remained relatively constant throughout this period (mandated access to facilities and associated costs), and those that have faded in and out of salience in relation to federal government actions (lawful access, copyright), or other events (Snowden's effect on privacy and surveillance discussions). Some of these recurring events (such as IETF and NANOG meetings) make recordings of presentations available, and reviewing the Telecom Summit's Regulatory Blockbuster for each year since 2010 has been particularly valuable in documenting concerns and shifts in Canadian telecom policy (Zajko, 2016b).

deals with additional domains of governance into which intermediaries' responsibilities have expanded, namely privacy, copyright, and security. The data used for these chapters varied depending on what was ultimately available to me; I utilized documents, recordings, and transcripts where these were public, and in other cases I sought to obtain my own data. My choice of case studies for these chapters was determined by their individual characteristics – namely ways in which the cases were exceptional, had a large transformative impact, or were representative of conditions and trends. However, data availability also played a large role in case selection, and I simply could not achieve sufficient access to some governing nodes to detail them as case studies, even if I wanted to.[36]

Government institutions proved to be a rich source of documents, whether generated by state or non-state actors (specifically those involved in regulatory processes and government consultations). Documents obtained from federal agencies through access to information (ATI) requests also provided valuable insight into government policy-making, the positions taken by different actors, and the processes through which governing nodes are coordinated. I reviewed tens of thousands of pages, from approximately one hundred relevant ATI files. These were most helpful in documenting processes that are normally hidden from public view, namely lawful access and cyber security. To limit the uncertainties and challenges of using the ATI system for research (see Larsen & Walby, 2012), and to collect data of broad scope, I requested ATI files that had already been disclosed pursuant to a previous request. Thankfully, documents pertaining to lawful access and cyber security are frequently requested by others, such as journalists looking

[36] For instance, I included the cases of O-Net, QNet, SuperNet, and Cybera in Chapter 2 because these are exceptional projects and institutions in Canadian telecom, but my access to data benefited from geographic proximity and the cooperation of participants. While I was able to communicate with two police officers about their lawful access experience, my efforts to gain access to a larger group of police participants through official channels would have resulted in conditions placed on my research which I could not accept. I therefore based my analysis of lawful access on documents from numerous access to information requests along with ISP perspectives.

for newsworthy information, whereas I was able to use the same documents to help understand these institutions and their relationships. Where I found noteworthy gaps in these documents that seemed relevant to my research question, I filed my own ATI requests for the missing information.[37]

While I analyzed documents where these were available, large areas of Canadian telecom remain poorly documented, including the topography and history of networks. Interviews (and informal discussions) were often necessary simply to establish basic facts about current and historical events. Attending events in Alberta, British Columbia and Ontario helped me make contact with individuals in these provinces who could provide further information through interviews. Other participants were recruited online, and interviewed over email or Skype. These expert interviews (see Bogner, Littig, & Menz, 2009; Szarycz, 2010) allowed me to fill gaps in documentary sources, and to gain a deeper understanding of my selected topics and themes. In total I carried out expert interviews with twenty eight participants, transcribed discussions at a two-day symposium with dozens of attendees (including individuals from local governments and the telecom industry), and had numerous informal discussions with industry executives, network operators, lawyers, consultants, police officers, and government officials. For one-on-one interviews, I used a semi-structured format tailored to the expertise of each participant. I did not aim for a representative sample, but instead sought specific information from individuals who I knew were in a unique position to provide it. Still, as is common with interview-based research, this process often resulted in participants raising unanticipated topics or providing surprising insights. The informal, conversational style of my expert interviews allowed me to build rapport in the course of my interaction with participants, and to follow these unexpected threads as they

[37] Specifically, three requests regarding CTCP and CSTAC, see Chapter 5.

arose.

I have tried to cover issues in Canadian telecom that are of national significance and relevance. Thankfully, a great deal of telecom governance in Canada takes place at the federal level, through institutions such as ISED and the CRTC. But telecom politics in Canada often have a strong local or regional dimension, with many ISPs serving a limited area, and relating to municipal, regional, and provincial governments. My field work was limited to three provinces, and the actors discussed in this dissertation are based mostly in Western Canada and Ontario. Issues particular to Quebec, Atlantic Canada, or the North are largely absent from this analysis, but the generalizability of my findings is strengthened by the federal institutions that provide a degree of uniformity across the telecom industry. For example, Quebec has recently been pursuing legislation to force ISPs to block certain gambling sites. This effort may be born of provincial political dynamics, but it must ultimately contend with the higher authority of the CRTC, which has national jurisdiction over telecom (Jackson, 2016b). Also, the trend of intermediation that underpins my argument is a broad and international one. While intermediation assumes some unique, local forms, intermediaries around the world are gaining in power, capacities, and political value as instruments of governance.

Who are the actors?: Intermediaries

I have repeatedly referred to both intermediaries and ISPs as being central to my analysis. It is important to clarify what I mean with these terms, since others have used different and inconsistent definitions. In this dissertation, an intermediary is any institutional actor that is positioned between two ends of a communication, occupying an intermediate position between users and internet services. This includes providers of internet connectivity such as ISPs, as well as OSPs that play a connective role (social networks that mediate communications between users, search engines that connect users to an organized Web). My primary focus is on providers of internet connectivity, but today's ISPs often have a broader role that encompasses OSP functions, such as providing content, webmail, or hosting. Of the institutional actors described in this section, the category of intermediaries is the broadest (see Winseck, 2015a), and the term has been adopted in internet governance discussions largely due to the fact that distinctions between different classes of service providers (such as those merely providing internet access and those providing additional services) have become blurred. At the same time, many of the diverse institutions categorized as intermediaries are subject to similar legal requirements or expectations on conduct (Edwards, 2011, p. 4). In Canadian telecom law, the “intermediary function” can be equated to acting as a “conduit” for a communication, with a “pure intermediary” acting “merely” as a conduit, and not otherwise exercising control or participating in the communication (*SOCAN v. CAIP*, 2004). In this dissertation, the term intermediary does not imply such a “pure” or “mere conduit” status, unless explicitly stated.

What follows is a list of some of the kinds of intermediaries referred to in this dissertation. However, it is important to note that a single actor can play multiple roles, and be characterized in a number of ways. For instance, Shaw is an incumbent cableco ISP that also acts as an OSP. The choice of which role or characteristic is foregrounded in my analysis depends on which role is of particular interest.

<u>Cableco:</u> A telecom company that developed out of a pre-internet cable television (co-axial cable or CATV) company. Contemporary Canadian examples include Rogers, Shaw, Vidéotron.

<u>FreeNet:</u> An ISP organized around a model of equitable connectivity: providing free, low-cost, or subsidized internet access to 'members'.

Incumbent: A telecom company that possessed facilities prior to liberalization. Incumbency is territorially-based, so that TELUS is an incumbent in Alberta and British Columbia, but not in Ontario, where Bell is the incumbent telco.

IISP – Independent Internet Service Provider: A non-incumbent ISP, or an ISP that originated following telecom liberalization. As with the 'independent' telephone companies of the twentieth century, the term can be quite misleading. This is because IISPs are often heavily-dependent on larger ISPs (usually the local incumbent) for upstream connectivity. Therefore, a more appropriate spelling might be (in)dependent internet service provider, or simply IISP.[38]

ISP – Internet Service Provider: An ISP is an institution that provides users, clients, or subscribers with an internet connection. Connectivity can be provided through network facilities owned by the ISP, or through leased access to facilities owned by another. ISPs have sometimes been differentiated into classes based on how central they are in the internet's topography (the center being occupied by Tier-1 ISPs or 'backbone' providers). ISPs can also be differentiated depending on the clients/users that they serve, with long-distance (international) carriers serving territorially-bounded ISPs, who in turn serve residential and business subscribers, or other sorts of users (see note 8 above).

Municipal Network/Municipal ISP: A publicly-owned municipal network. This may be a 'community network', created by individuals organizing as a group to improve connectivity in their locale (O-Net), or it may be the result of a municipal government finding a better way to meet its networking requirements (QNet, City of Calgary).

OSP – Online Service Provider: An institution that provides a service that is accessible online, often through a website (including Facebook and Google).

REN – Research and Education Network: A network that provides connectivity to research and education institutions, such as universities, but which may also have a broader function in promoting entrepreneurship and innovation (see Chapter 2). Typically, RENs are publicly-funded. In Canada, there are twelve provincial and territorial RENs (also known as Optical Regional Advanced Networks, or ORANs), operated by institutions such as BCNET and Cybera. These are interconnected at the national level through the National Research and Education Network (NREN), which is operated by CANARIE.

Telco: A telecom company that developed out of a pre-internet telephone company. Contemporary Canadian examples include Bell, TELUS, SaskTel. At the CRTC, these companies are often classified as Incumbent Local Exchange Carriers (ILECs).

Who are the actors?: Government institutions

Intermediaries govern our data flows, but who governs the intermediaries? The list of

[38] I appreciate Benjamin Klass's help in working through this categorization.

governing institutions and groups is a long one, and varies according to an intermediary's organizational structure. There are controls internal to the organization (self-governance), shareholder or 'member' control, internet governance organization like ICANN and Regional Internet Registries (RIRs) that play limited but important roles, and industry associations that can influence (but not mandate) member organizations. Finally, we must consider the various state and quasi-public agencies to which intermediaries are accountable, and which often exercise sovereign authority over a domain. It is this final category of government actors which are principally important in a national context and are the main focus of this dissertation.

At the federal level in Canada, the job of governing communications networks in the public interest is largely the responsibility of the CRTC, particularly through its administration of the Telecommunications Act. The CRTC is a quasi-judicial body whose commissioners rule on a variety of issues brought to them, primarily by telecom companies taking issue with regulations or the behavior of competitors. The national public interest in telecommunications is also decided by the elected federal government, and the federal Cabinet can exercise its authority over the CRTC (by issuing policy directions and orders-in-council).[39] Other relevant federal institutions are Innovation, Science and Economic Development Canada (formerly Industry Canada), which among its many responsibilities manages wireless spectrum in Canada, the Copyright Board, which has the power to require ISPs to pay royalties to copyright owners, and the Competition Bureau which regulates anti-competitive conduct.

However, there are numerous other governing nodes in Canada that exercise meaningful

[39] The CRTC is sometimes described as being “arm's-length” from government (Lasalle, 2012; Winseck, 2014), but the actual distance depends on the government of the day. There have been periods in the CRTC's history where it was more regularly overruled and directed by government (Winseck, 1998, pp. 236–238), and the CRTC generally tries to align itself with the direction set by government. It should also be noted that decisions of the CRTC can be appealed to Federal Court.

control over internet intermediaries towards public ends – even if these publics are more circumscribed than that of the nation. A number of provinces have addressed the lack of federal broadband projects with their own provincial initiatives. Some municipalities and First Nations have taken an active role in deploying networks to serve their residents. There are also regional initiatives that have arisen when a number of communities have collaborated out of common interest. In Canada, internet governance has effectively become a concern for all levels of government.

Setting the scene for the current milieu

Now that I have laid out how this dissertation is organized, introduced my methods and theoretical commitments, as well as the actors featured in the following chapters, I must ground Canada's current telecom politics in historical context. The following chapter explains how today's ISPs and the political economy of telecom developed from pre-internet arrangements of actors and public policies. These policies installed government agencies as regulators, constrained and protected the twentieth-century's telecom monopolies, and then replaced the monopoly regime with liberalization. However, despite liberalization, the legacies of earlier eras continue to shape the present.

Chapter 1: The history and political economy of Canadian intermediaries

Thus commerce will be stimulated, time and money will be saved, friendship will be promoted; sociability will be encouraged and these ever extending wires will not only bring pecuniary profits to the people... but will also carry into hundreds and thousands of hearts and homes throughout this broad land cheering messages of hope, encouragement, grace and goodwill.
-John T. Moore, 1907 (Cashman, 1972, p. 141)[40]

To understand the forces governing internet intermediaries in Canada, as well as the current configuration of actors and their power relations (the political economy of internet access),[41] it is instructive to briefly look at the historical development of the country's telecom networks. The use of private intermediaries as instruments of public policy is hardly a recent invention, and was a key part of the "public service liberalism" (Stone, 1991) that predominated as the governing rationality of North American telecom from the 1800s until the 1990s. Many have identified the period that has followed as the neoliberal era, but it is more accurately described as a form of regulatory capitalism that shifted the public service obligations of telecom companies. This was a shift toward liberalization and market competition, but not deregulation. Instead, regulation became seen as the key to promoting competition, and dealing with its consequences. Canada's internet topography and the political economy of telecom are grounded in these historical transformations.

The internet is carried over a material infrastructure (cables, poles, towers and switches), much of which was constructed by telcos and cablecos in a pre-internet era. Internet regulations

[40] John T. Moore was a politician, telephony pioneer and supporter of publicly-owned telephones in Alberta. The excerpt is from an address to the Alberta Legislature on February 14, 1907

[41] I use the term political economy here in the narrower sense identified by Mosco (2009, p. 2), referring to "the social relations, particularly the power relations, that mutually constitute the production, distribution, and consumption of [communication] resources".

drew on many principles and precedents from the regulatory history of telecom and telephony,[42] and telecom liberalization in the 1990s inherited the previous era's monopolies as incumbents. This chapter traces these developments and their role in shaping the political economy of the present, providing additional context to contemporary actors and policies. The objective is to explain how Canada's telecom networks are governed following liberalization, a term which cannot be confused with neoliberalism. Strong arguments for a neoliberal approach to telecom policy have been made by some in government and private industry, but various kinds of state regulation have remained in place or expanded into new domains. As in the days of corporations explicitly chartered to serve the public interest, today's intermediaries are required to fulfill certain public obligations. Some, like responsibilities concerning internet child exploitation and cyber attacks, are a response to internet-era social problems enabled by technological change, while others, like the mandated access regime, are meant to structure competitive relations following liberalization. However, many of the public policy issues in Canadian telecom have deep roots in a previous era of telephony and monopoly.

Telephony and monopoly

The early days of telephony in Canada saw a proliferation of local exchanges, beginning in the late 1870s. However, in the span of a few years the Bell Telephone Company of Canada acquired a telephone monopoly in much of the country, first buying up the local exchanges, and subsequently connecting them with long-distance lines (Rens, 2001). The company's rise was

[42] The telephone was preceded by the telegraph by several decades, and the two technologies were closely related in their functionality. Telephony and telegraphy shared an evolving regulatory environment in the mid-1800s, and the spread of both technologies was frequently supported and driven by the same companies (Winseck, 1998). However, I am limiting this historical narrative to telephony for the sake of simplicity.

due in large part to its close relationship with the American Bell Telephone Company (later AT&T), and its success in petitioning the federal government to grant Bell a charter to develop its telephone network across much of Canada.[43] The *Bell Telephone Company of Canada Act* that incorporated Bell in 1880[44] also had the effect of asserting Ottawa's regulatory control over telephony, although this control was far from absolute, since lower levels of government still governed telephone systems in their jurisdictions. While provinces and municipalities could operate their own telephone networks, they were prohibited from appropriating parts of Bell's network, or interfering with rights granted to Bell under its charter. These rights included access to public rights-of-way (such as streets and bridges) along which its network could expand (Babe, 1990, p. 68; Government of Canada, 1880; Martin, 1991, p. 23; Winseck, 1995, 1998, pp. 119–120), and which recurrently became sources of conflict between Bell and municipalities (MacDougall, 2013, Chapter 1).[45] In numerous cases, these conflicts were overcome or preempted by exclusive franchise agreements that Bell was able to negotiate with municipalities (MacDougall, 2013, pp. 45–47), granting the company dozens of municipal monopolies. Bell's early success was therefore not due to some inexorable pull towards a “natural monopoly” in telephone service (as was sometimes claimed in the interests of limiting competition, see Dagger, 1915), but rather "an outcome both of government privilege and of aggressive and frequently predatory business practices" (Babe, 1990, p. 89). These business practices included a refusal to

[43] British Columbia was a notable exception to Bell's early ambitions (Rens, 2001, pp. 75–78), and the Northwest Territories (which until 1905 encompassed the lands that would become Alberta and Saskatchewan) was a vast territory in which Bell's charter was disputed (MacDougall, 2013, p. 186).

[44] The *Act* was an incredible accomplishment for Bell and its head, Charles Sise, who achieved it without any significant political opposition through “lightning” speed (Rens, 2001, pp. 67–68). For Babe (1990, pp. 69–70), the unsolved “riddle” of this accomplishment is that the company's American connections never became a point of political debate, given the federal government's nationalistic orientation.

[45] This was part of a larger conflict between utility companies (many of whom sought a charter similar to Bell’s) and municipalities over control of infrastructure in Canada’s rapidly developing cities (Armstrong & Nelles, 1986, Chapters 7–8).

interconnect with smaller telephone companies, whom Bell saw as competitors, and would buy out when possible in well-populated areas (Rens, 2001, p. 88).[46]

However, Bell was largely uninterested in expanding its network to less-profitable rural areas (MacDougall, 2013, p. 123), and was more accommodating with rural companies that it did not see as competition (Babe, 1990, p. 115; Rens, 2001, p. 90). Many villages and some municipalities constructed their own telephone systems to meet local communication needs.[47] Some provinces nationalized these services along with the connections between exchanges. Prairie farmers proved particularly independent and resistant to Bell's westerly expansion.[48] Farmers depended on communication in areas where low population density made building networks uneconomical, and formed cooperatives to deal with various collective challenges, including communications. Urban populist movements also developed calling for better, cheaper service. When Edmonton became a municipality in 1904, it immediately held a referendum wherein residents overwhelmingly voted to municipalize telephone service (Cashman, 1972, pp. 119–121; Rens, 2001, p. 95). Shortly thereafter, Manitoba threatened to build a parallel network against Bell, compelling the company to sell its provincial assets to the government (Armstrong & Nelles, 1986, pp. 177–185). Alberta followed in 1908, buying Bell's 19 local exchanges and 18 long-distance exchanges in a political climate characterized by western pride and opposition to the eastern "monopoly" (Cashman, 1972, pp. 137–141; Rens, 2001, p. 110).[49]

[46] In a few cases, the company also offered discounted or free telephone service for as long as required to eliminate a municipal rival (MacDougall, 2013, pp. 43–44; Rens, 2001, p. 86).

[47] Rural systems were often private, established by various kinds of businessmen or doctors (Babe, 1990, pp. 82–83).

[48] The Maritimes also gained independence from the Bell system in the 1880s (Rens, 2001, pp. 81-84).

[49] Saskatchewan followed a similar path in 1909 (Dagger, 1915; Rens, 2001, p. 111).

In Ottawa, municipal dissatisfaction with Bell and calls for government intervention culminated in a 1905 Select Committee to investigate telephones (the Mulock Committee), which heard from various parties complaining about Bell's practices, some of whom[50] argued for the nationalization of long-distance telephone service and municipal control over local service. In its defence, Bell could argue that it was working in the interests of the "general public" (Armstrong & Nelles, 1986, p. 171; Babe, 1990, p. 100), as its charter had been extended and revised in 1882 to define the company as working "for the general advantage of Canada" (Government of Canada, 1882, sec. 4; see Rens, 2001, p. 75). The company's private interests had thereby been explicitly defined as benefiting the Canadian public, enabling the company's spokespersons to wrap Bell in nationalistic rhetoric, and helping provide some legal protection against municipalities seeking control over Bell's poles and wires (MacDougall, 2013, p. 34). However, Bell's charter could not guarantee that the company would be free from federal government regulation, or the threat of nationalization. Critics could even turn the language of its charter against Bell when pointing out its neglect of rural areas (Dagger, 1915, p. 309).[51]

The Mulock Committee of 1905 did not immediately result in significant changes to the political economy of telephony, securing Bell's position as an incumbent in much of Canada, and rejecting the possibility of nationalization. However, by 1906 Parliament decided that the company would be regulated by a permanent and neutral commission.[52] Since Bell had an

[50] Most notably Francis Dagger, a central figure advocating for municipalities and against the Bell monopoly in this period (Armstrong & Nelles, 1986, pp. 167–169; Winseck, 1998, p. 129).

[51] Ultimately, Bell relied less on legal precedent or its charter to make its case before the Mulock Committee, and instead emphasized technical arguments for maintaining both local and long-distance service under a single system, which would be best left under its expert control (MacDougall, 2013, pp. 180–182). Bell's monopoly was justified on the basis of technical necessity as dictated by the inherent properties of telephony.

[52] Rens (2001, p. 99) characterizes the move as a "tacit exchange of monopoly for regulation". The regulator would be the Board of Railway Commissioners (BRC), and in 1908, an amendment to the Railway Act extended the BRC's powers over all telecom (telephone and telegraph) companies under federal jurisdiction. The

effective monopoly on long-distance service in much of Canada, its new regulator deprived Bell of the ability to unilaterally refuse interconnection with other companies (interconnection was crucial for local telephone systems to make calls beyond their local areas). The regulatory commission could also examine Bell's costs in order to set “just and reasonable” interconnection rates (which did not prevent these costs or their disclosure from being a source of dispute, see Rens, 2001, Chapter 15).[53]

The installation of neutral regulatory commission to oversee telephony established a framework that spread across the U.S. at roughly the same time,[54] where Bell companies also became stewards of the public interest, were regulated by independent commissions, and in exchange received certain state guarantees or protections (like monopoly rights). In both countries, this “public service liberalism” (Stone, 1991) gave way to regulatory capitalism in the 1980s and 90s, but many of its fundamental dynamics have continued today under the CRTC. For instance, the wholesale internet regime described in Chapter 3 mandates interconnection between incumbents and smaller intermediaries, and leaves the two perpetually battling before the CRTC over tariffed rates and what incumbents deserve to be paid for access to their facilities. But while the wholesale internet regime has been justified primarily as a policy to enable competition, mandated interconnection in early telephony was justified by the “public interest”

consequences of this move included granting more power to municipalities, and regulating interconnection between Bell and the smaller (or independent) telephone companies. The BRC was renamed the Canadian Transport Commission (CTC) in 1938.

[53] Interconnection rates become the key point of contention before the BRC in subsequent years, with the Board deciding questions such as whether Bell should be compensated for business it lost to its competitors through interconnection, and making distinctions between which companies were competitors to Bell and which were non-competitors (with companies deemed to be competing subject to higher rates, see Babe, 1990, pp. 116–119; Rens, 2001, p. 102; Winseck, 1998, pp. 129–135). Indemnification became a key point of dispute between Bell and the Canadian Independent Telephone Association in 1917, and the dispute carried over into the House of Commons and Senate until new legislation was passed in Bell's favor in 1919 (Babe, 1990, pp. 119–121).

[54] Interestingly, Canada's regulatory regime also influenced the development of US telephone regulation in 1910 (Rens, 2001, p. 103).

of connecting the subscribers of different companies (Canadian Independent Telephone Association, 1911, p. 483).

Competition in telephony was actually seen as undesirable for much of the twentieth century in Canada,[55] but regulators did work to restrict the anti-competitive practices of telecom companies under another doctrine which would come to be relevant to internet intermediaries, known as "common carriage" (K. G. Wilson, 2000, pp. 50–51; Winseck, 2015a, pp. 489–492).[56] In short, common carriers are transportation and communications institutions that are seen as serving the public, and are thereby prohibited from refusing service or discriminating between customers. Railway companies were required to carry freight from different clients on equal terms, and telecom companies (who shared the same regulators as the railway companies for much of the twentieth century in Canada) were likewise eventually required to transmit communications without interference or discrimination.[57]

In effect, common carriage meant that any institution that acted as a 'carrier' of information (what would come to be called a 'mere conduit') was barred from doing anything

[55] Rather than seeking to have multiple companies operating in a given market, the BRC actively took steps to suppress competition by discriminating against companies seen to be competing with Bell (Rens, 2001, p. 102). The undesirability of competition between telephone companies (what the Chief Commissioner of the BRC called the "evils of telephone duplication" in 1914, see Babe, 1990, p. 119) would be justified through the doctrine of "natural monopoly" (Dagger, 1910), which held that competition in telephones was undesirable and unsustainable (Babe, 1990, p. 137; Winseck, 1998, pp. 7–9). This principle was not only espoused by Bell and its regulators, but was also echoed by municipal governments, which actively opposed competing telephone companies operating over city streets (MacDougall, 2013, p. 128). By 1925 all direct competition with Bell had been eliminated, and the number of independent companies serving rural areas gradually dwindled through the twentieth century (Babe, 1990, pp. 116, 121–124, 135).

[56] Precursors to common carriage regulations governed British transportation networks in the 1700s (and have been identified as early as the Roman Empire), before crossing into the North American context in the 1800s to deal with railroads and telegraphy (Cherry, 2015, pp. 469–470; Noam, 1994, pp. 436–437; Stone, 1991, Chapter 2).

[57] While the analogy between transporting parcels and communications was rejected by Canadian courts in the nineteenth century (Winseck, 1998, pp. 100–103), the issue came to a head as a result of Canadian Pacific charging higher rates to carry certain news services in 1907, so as to advantage its relationship with Associated Press (Babe, 1990, pp. 57–59; Rens, 2001, pp. 34–36; Winseck, 1998, pp. 104–107). The BRC therefore imposed rate regulation on telegraph companies in 1910, and the common carrier principle was subsequently extended to telephony.

other than ensuring that this information reached its destination, and obliged to treat all communications on an even-handed basis. Previously, telegraph companies had been intimately involved in the news-gathering process, and gave preferential treatment to their press partners. Now they were constrained "as public services with an exclusively technical vocation", with common carriage becoming "the cornerstone of all Canadian rights in communications" (Rens, 2001, p. 36). The legacy of this regulatory principle continues to have significant implication for internet intermediaries, affecting copyright enforcement, net neutrality, interconnections between ISPs, and the extent to which incumbent ISPs can take advantage of vertical integration.

The gradual breakdown of system integrity and natural monopoly

Power relations in Canadian telecom largely stabilized after the onset of the 1920s, with municipal tension easing and the majority of independent telcos gradually going out of business. Bell and the provincial telcos consolidated their territories,[58] and found ample reasons to cooperate as they became interconnected parts of a "pan-Canadian" network (Rens, 2001, p. 251).[59] The principle of common carriage became well established and adhered to. Finally, as telephone connectivity became indispensable to modern life, the principle of "universal service" or universalism (Birdsall, 2000) gradually developed, with the public policy goal of providing service to all Canadians. This became a key justification for natural monopoly, since it was argued that universal service was only possible through a large monopoly that could use profits

[58] What Wilson (2000, p. 73) characterizes as the "Canadian monopoly mosaic".

[59] In the 1920s, seven telco incumbents formed the Telephone Association of Canada, and subsequently went about building the Trans-Canada Telephone System (TCTS) – a long-distance line that would help unify Canadian telephony. Each company took responsibility for the TCTS in its area, but Bell played an essential leadership role (Armstrong & Nelles, 1986, p. 292; Rens, 2001, pp. 203–212; Rideout, 2003, pp. 27–28).

from urban areas to subsidize more expensive rural lines (Babe, 1990, p. 139; K. G. Wilson, 2000, pp. 59–61).

Another key principle justifying the natural monopoly of the telcos was that of "system integrity" (Babe, 1990, p. 143), which had been employed so effectively during the Mulock Committee of 1905, and was likewise the basis of AT&T's argument in the US for a single, centralized telephone system under its control (MacDougall, 2013, Chapter 6; Stone, 1991, pp. 220–225). It was argued, and widely accepted, that this control should extend 'end-to-end' through the network in order to produce maximum benefits. A network cobbled together from multiple heterogeneous parts, or used to connect whatever assorted devices customers decided to plug into it, was seen as unwieldy and dangerous.

Today, we can recognize this argument as contradicting a key principle that has often been identified as underpinning the architecture of the internet. The internet's rather different "end-to-end" principle states that most features of the network should be implemented through the computers at either end of the network, with everything in between limited to faithfully carrying data packets to their destination (Lemley & Lessig, 2001; Zittrain, 2008, p. 31). In other words, the 'intelligence' of the network should be at the endpoints, with 'dumb pipes' in-between, and this simplicity at the core of the network allows various kinds of systems to interconnect using internet protocols. In contrast, natural monopoly in telephony was justified by the need for centralized control over a singular system, including the telephones at the endpoints. This argument was less sustainable as it became clear that whatever the transmission medium (whether telephone cables, CATV, or wireless), all were multi-purpose telecom networks, rather than discrete, specialized systems.

During the 1970s the technological determinism that had concealed the underlying political economy of telecom (see MacDougall, 2013) began to break down. For example, while cable was eventually deployed throughout urban Canada and capable of carrying far greater volumes of information than telco "twisted-pair" copper lines, cable systems were prohibited (through their agreements with telcos)[60] from stepping outside of narrowly defined role as carriers of television signals (Babe, 1975, Chapter 7, 1990, pp. 215–216; Winseck, 1998, pp. 183–184). Many of these restrictions were relaxed by regulators in the mid-1970s, first under the Canadian Transport Commission (CTC) and then the CRTC (Babe, 2011, p. 124). While terms such as 'information highway' and 'internet' had yet to be brought into use, it became increasingly evident that telecom networks, whether operated by telcos or cablecos, acted fundamentally as carriers of information, and that attempts to limit them to particular uses or configurations were not dictated by technological necessity. This realization was slow to spread, in large part because incumbent telcos and cablecos were keen to preserve the status quo (Winseck, 1998). Monopoly control over telecom stood as an obstacle to a growing industry developing new forms of data networking, and these forces were less likely to conform to the established order. Bell was first challenged over end-to-end control and system integrity in the 1950s,[61] and by 1968 its regulator

[60] While cable networks (cablecos) eventually became the telcos' main competitors in the internet era, when CATV was first deployed in the 1950s it was heavily dependent on telco infrastructure (such as telephone company poles, or entire systems built by telcos and then leased to the cablecos). Therefore, while the development of cable networks in the mid-twentieth century had the potential to radically transform the nature of communications networks in Canada, this potential was kept in check by the incumbent telcos who had no desire to upend the comfortable state of Canada's telecom regime. Until liberalization, cablecos were also comfortable serving their own niche markets, with no desire to compete against the much larger telcos, and keen to be exempt from greater government regulation, including the mandate of universal service (Winseck, 1998, pp. 185–186).

[61] In 1955 a small company tried to retail a device to kill germs in the telephone receiver by emitting ultraviolet rays. Bell successfully blocked the invention in court, as the company had the power to prevent any devices from connecting to its network without permission. However, through the 1950s Bell did grant permission for numerous other kinds of devices (such as radar stations and medical equipment) to utilize its network (Rens, 2001, pp. 292–293). In contrast, the Hush-A-Phone in the U.S. resulted in AT&T being ordered to allow

gained the power to decide what devices could be attached to the network.[62] The same year, Bell successfully lobbied government to broaden its charter from "telephones" to "telecommunications" (Babe, 1990, pp. 184–186). Bell knew that once its monopoly control was weakened, it would have to compete with other companies wishing to use its network for applications such as time-sharing on mainframe computers.[63] For its part, the company tried to forestall changes to the regulatory status quo as long as possible (Mussio, 2001, p. 225), while developing its own telecom service offerings to feed customers' demands for data communications.[64]

A major regulatory shift occurred in 1976,[65] as the responsibility for telecom regulation at the federal level was transferred from the CTC to the CRTC. The move stemmed in part from the perception that the CTC was unable or unwilling to keep up with the task of regulating the telcos, that its process worked in the companies' favor, and that its exclusive nature was at odds with

subscribers to attach the privacy-enabling device in 1956, opening the door to other devices such as fax machines, and eventually the dial-up modem (Zittrain, 2008, pp. 21–22).

[62] In 1968 Parliament amended Bell's charter, empowering the CTC to judge what sorts of attachments to the Bell network were "reasonable" (Babe, 1990, p. 145). However, the CTC did not push Bell to open its network, and telco incumbents continued to oppose any relaxation of the conditions under which they would allow interconnection between their networks and other devices or systems. Bell opposed such interconnection on the grounds of the public interest, and its need to "ensure the safety of employees and customers" by guarding against "electronic pollution and interference" (as cited in Mussio, 2001, p. 178). Western provinces were also strongly opposed to anything that might threaten "the essential need for a monopoly environment in the provision of telecommunications services" (as cited in Mussio, 2001, p. 182). But by the mid 1970s the federal government, under pressure from IT companies such as IBM and the Electronic Industries Association of Canada, came to see interconnection as a crucial way to promote innovation and to maximize the public benefits of data communications services (Mussio, 2001, pp. 179–181).

[63] Prior to the personal computers (PCs) of the 1980s, it was imagined that the future of data communications would be to connect distributed "dumb" terminals with centralized computers. The initial purpose of ARPANET, the internet's predecessor, was to allow time-sharing of expensive computing resources, so that researchers could access mainframes remotely (Hafner & Lyon, 1996; Leiner et al., 2009, p. 25). As Mussio (2001, Chapter 7) documents, the dream of a national computer utility was pursued in Canada from the late 1960s until the mid 1970s along some related lines, until divergent interests in industry and the lack of a coherent government position led to the project being dropped. At roughly the same time, efforts were under way to create a Canadian version of ARPANET (CA*net Institute, 2001, pp. 16–23).

[64] In 1973, Bell began offering Dataroute through the TCTS to serve the data transmission needs of banks and other large corporations. In 1978 Bell began offering its DATAPAC service - one of the earliest commercially-available uses of packet-switching technology (Bostelaar, 2009; CA*net Institute, 2001, p. 24).

[65] Following 1975's passage of the *CRTC Act*.

democratic politics (Babe, 1990, pp. 164–168; Stevens, 1976; Winseck, 1998, p. 61). Whereas the CTC had refused public participation in its hearings, the CRTC promised to take a broader view of the public interest (Winseck, 1998, p. 61), holding less-formal hearings that were open to public (“CRTC warned by Bell against being too free with data for public,” 1976; Janisch, 1979, pp. 91–92; Stevens, 1976; Winseck, 1998, pp. 61–62). While the CRTC did prove to be more open to hearing from voices that had previously been excluded from regulatory hearings, questions remained about just who would represent the public before the CRTC, and about the best way to encourage public participation in its decision-making. These issues continue to challenge the Commission to this day.

Very quickly after it stepped into its new role, the CRTC's actions signaled a change in how it would regulate the telcos under its jurisdiction, including a broader interpretation of its regulatory mandate than that which had been adopted by the CTC (Schultz, 1999, pp. 40–41). The issue of “terminal attachments” (endpoint devices connected to the network by customers) came up again in 1976, and the Commission found Bell's actions to be discriminatory, dismissing the company's arguments for system integrity (Babe, 1990, pp. 147–148; “CRTC decision held a precedent for additional challenges to Bell,” 1977; Winseck, 1998, pp. 195–196). Thereafter, the CRTC would compel the common carriers to allow new kinds of devices to be connected to their networks.[66] These intermediaries were no longer just obliged to faithfully carry customers'

[66] For instance, in Telecom Decision CRTC 89-5, and in the interest of promoting competition, the Commission ordered Bell and BC Tel to open the Dataroute network (see note 64 above) to terminal attachments, and to provide sufficient information about how the network operated for the design of such devices (see Barnes, 1986). It is also important to note that while Bell was disputing the issue of terminal attachments before the CRTC, the federal government (Department of Communications) was pursuing a voluntary and cooperative approach to terminal attachments that included both common carriers and equipment manufacturers (K. G. Wilson, 2000, pp. 190–191).

communications from endpoint to endpoint, but also to give up control over what those endpoints were connected to.

The issue of terminal attachments was just one in a series of moves towards greater liberalization of the telecom industry in Canada. When Bell asked the CRTC to rule on the issue of terminal attachments again in 1979, the company's argument was no longer the narrow concern over system integrity, but the broader question of whether allowing greater competition in terminal attachments was in the public interest (K. G. Wilson, 2000, pp. 195–197). Technical arguments gave way to other concerns over the consequences of telecom liberalization, including economic impacts on the common carriers, the social impacts to unions and universal service objectives, and political struggles over jurisdiction between the federal government and the provinces. The eventual result would be the breakup of the established monopoly regime, occurring just prior to the arrival of the commercial internet and the first Canadian ISPs. This allowed various small intermediaries to take advantage of recently 'opened' networks to provide budding internet services, but also marked the beginning of an era in which it made sense to refer to preexisting telcos and cablecos as 'incumbents'. In a newly competitive, less restrictive, and privatized[67] marketplace, the field would be open to a host of newcomers. But in the end, the many decades through which incumbents had established themselves would accord them a host of advantages, and compensating for these advantages would require constant regulatory balancing on the part of the CRTC.

[67] In the case of government-owned telco networks, as in Manitoba and Alberta.

Regulatory liberalization

In brief, liberalization is a form of state intervention that opens the telecom industry to competition and aims to increase the number of competitors (Mosco, 2009, p. 177). While often described as 'deregulation', this terminology is misleading and self-serving, since it suggests that regulation gives way to the ascendancy of the market. Instead, liberalization involves choices between different forms of market regulation (Mosco, 2009, p. 176) in which the state often takes an active role to further different interests, rather than the removal of regulation. The state might continue to exercise power to constrain or direct the market towards values in the public interest, such as universal service and affordability. However, liberalization typically means less state involvement in rate-setting, a sacrifice of the universal service objective, and new kinds of state intervention to encourage increased competition. The state retains the power to intervene where competition is seen to be inadequate, when competitors abuse their positions, or in instances of "market failure" (Rideout, 2003, p. 65). These forms of market regulation (or "regulated competition", see Romaniuk & Janisch, 1986, p. 612) have kept the CRTC quite busy in the era following liberalization (see Chapter 3). While the goal may be to create a reliance on market forces that requires only minor regulatory intervention, the state has been unable to fade from the scene as much as policy makers have wanted. Telecom liberalization is not simply a process that Canada underwent in the 1980s and 1990s; it is a continuous mode of governance that presents no end of problems to be solved by the state. The end goal may be deregulation, and a reliance on market forces to drive efficiency, competition, and choice for consumers. However, in the never-ending interim, the market must be regularly adjusted, recalibrated, and its players repositioned.

Liberalization has been a gradual and uneven process. Federal concerns about the duplication of facilities still surfaced in the mid-1980s (Babe, 1990, p. 240) – a decade characterized by the lack of coherent federal policy on telecom liberalization (Romaniuk & Janisch, 1986) despite some significant steps taken in that direction. Any nation-wide liberalization implicated both provincial and federal governments, but provinces disagreed with the form of liberalization being promoted by federal institutions,[68] and opposed claims of federal jurisdiction over provincial telecom companies (Janisch & Schultz, 1991; K. G. Wilson, 2000, pp. 180–185). Opposition to liberalization also came from labour unions, several interest groups (including anti-poverty, consumer, and public interest organizations), and some rural subscribers (Rideout, 2003; Winseck, 1998, pp. 196–198, 234). Serious disagreements occurred between the CRTC, Department of Communications (now ISED) and federal Cabinet over the shape of liberalization in the late 1980s and early 1990s. Since the CRTC can effectively have its decisions overruled by Cabinet, the commission was ultimately brought into line with its political masters' "de facto" competitive telecom policy (Winseck, 1998, pp. 235–238). But there was no grand plan or explicit policy of liberalization in this period. Instead, the slow path to liberalization was built through the alignment and accumulation of individual regulatory decisions (K. G. Wilson, 2000, p. 63), such as opening up competition in terminal attachments, data services, as well as long-distance and local telephone service (Schultz, 1999, pp. 42–45; K. G. Wilson, 2000, Chapters 7–8; Winseck, 1998, Chapter 6). Liberalization was also spurred on

[68] Specifically, Manitoba and Saskatchewan had been upgrading their core networks with significant broadband expansions and wished to retain monopoly control over this infrastructure, while opening services to competition (Winseck, 1998, p. 197).

by related developments in the U.S., and the desire to make Canadian carriers "competitive" in the evolving North American market (K. G. Wilson, 2000, pp. 173–175).[69]

Telecom liberalization through the 1980s and 1990s also coincided with and was complemented by the privatization of (wholly and partly) state-owned intermediaries, including the provincial telcos in Alberta and Manitoba, along with NortwesTel, Terra Nova, Telesat Canada, and Teleglobe (K. G. Wilson, 2000, Chapter 7; Winseck, 1998, pp. 228–229). With the exception of a small number of municipally-owned intermediaries and specialized networks such as those used for research and education (see Chapter 2), a policy consensus formed around the idea that the state had no business being in the telecom business. Future state involvement in telecom would be limited to setting and adjusting the "rules of the game" (Mussio, 2001, p. 227), contracting out public policy to the private sector, and public-private partnerships.

Finally, telecom liberalization was also a process in which regulatory power was centralized and consolidated as a federal regime with explicitly stated policy objectives (Winseck, 1998, pp. 234–241). Principally, this was achieved by a Supreme Court decision that affirmed the CRTC's jurisdiction over provincial telcos in 1989 (Janisch & Schultz, 1991, pp. 171–175; K. G. Wilson, 2000, pp. 183–185; Winseck, 1998, p. 239),[70] and the *Telecommunications Act* of 1993 (Rideout, 2003, pp. 139–147; K. G. Wilson, 2000, pp. 228–233; Winseck, 1998, p. 238). Previously, the CRTC worked under a vague mandate to ensure that rates were "just and reasonable" and to prevent "unjust discrimination" (Romaniuk & Janisch, 1986, p. 585; K. G. Wilson, 2000, p. 61). The Commission had taken an ad-hoc

[69] Telecom liberalization, particularly on the issue of long-distance competition, was also strongly encouraged by corporate telecom users and business lobby groups (Rideout, 2003; K. G. Wilson, 2000, pp. 204–206).

[70] Previously, while the federal government could have chosen to assert its authority over telecom, provincial telcos were left alone due to "provincial sensitivities" (Winseck, 1998, pp. 212, 239–241)
.

approach to regulating competition and interconnection. Now, the CRTC was finally granted a legislative mandate to regulate telecom, along with an explicit list of objectives to work towards, and truly national jurisdiction over intermediaries. While the *Telecommunications Act* was an articulation and formalization of a national policy of telecom liberalization after it had become irreversible, it also centralized regulatory authority under the CRTC, and therefore, the federal government.

Liberalization turned monopoly telcos and consolidated cablecos into incumbents, and opened the field to new competitors that might challenge them in their established markets, or in new services such as internet access. Ultimately however, incumbency would prove decisive. While the CRTC pried open access to incumbent networks one piece at a time, the intent was never to dethrone these champions. Instead, the regulator deprived incumbents of certain methods of control over their infrastructure, and saddled them with responsibilities to facilitate new participants in the market. New competitors that might otherwise be crushed by incumbent power would be accorded some regulatory protection, but it was also imagined that the incumbents would vigorously compete with one another. These twentieth-century masters of their respective domains, would now be unmoored from their mutually-agreed upon territories. Bell for instance, was free to come west, and TELUS (formed through the merger of Alberta and BC's telco monopolies) could build networks and fight for customers in Bell's traditional Ontario and Quebec territories. The extent to which these incumbents actually do compete with one another is the source of much debate, and will be taken up in Chapter 3.

Liberalization and neoliberalism

Canada undertook telecom liberalization at roughly the same time as much of the rest of the world. This period also overlapped with the opening of public access to internet (although at the time, it was often referred to in other terms, such as the 'information highway'), and the rise of the first commercial ISPs. Indeed, the development of the internet in each country was intimately related to, or developed on the basis of telecom liberalization (Kushida, 2015).

In an international perspective, Canada's commitment to market-based telecom liberalism has been exceptionally strong (Birdsall, 2000). Academic critique has often identified the dominant post-liberalization rationality of Canadian telecom policy as neoliberalism (Birdsall, 2000; Kozak, 2010; Rideout, 2003), and neoliberalism has become an influential narrative and theoretical explanation of the international transformations in governance that have taken place since the late 1970s. While the term developed increasingly broad and contradictory meanings (Venugopal, 2015),[71] a consistently-emphasized characteristic of neoliberalism as an approach to public policy has been deregulation, with the neoliberal state retreating and governing less as market forces take over. However, this narrative has often been inconsistent with actual policy developments, including in telecom. As documented by Vogel's (1996) *Freer Markets, More Rules*, privatization and liberalization have typically been accompanied by a proliferation of regulations and regulatory institutions. It is therefore important to distinguish between neoliberalism as a set of claims or recommended public policy positions, and the actual set of

[71] This critique is not lost on some scholars of neoliberalism. For example, Brown describes neoliberalism as a "loose and shifting signifier" that is "globally ubiquitous, yet disunified and nonidentical with itself in space and over time" (2015, pp. 20–21). Brown claims to analyze neoliberalism's "current iteration" rather than its "essential and global truth" (2015, p. 21), but the term is useful precisely because it can identify local manifestations of a global project with some essential characteristics. While scholars of neoliberalism typically agree that the extension of market logic to new domains is one of these essential characteristics, other contours of neoliberalism (such as the extension of individual responsibility or the shrinking of the state) are more controversial.

policy developments that occurred during what is supposed to be the “neoliberal era”. As Braithwaite (2008, pp. 8–10) argues, the “neoliberal policy package” was never an accurate way of describing what happened in countries like the U.S., U.K. and Canada during this period. While small government and deregulation was certainly what some people (particularly in the private sector) wanted, governments in these countries proved adept at deploying the rhetoric of neoliberalism and practicing extensive domestic regulation.

Contrary to the prescriptions favored by neoliberal advocates, the Canadian state maintains an active role in regulating the marketplace for telecom services, and a number of pre-internet regulatory distinctions continue to restrict the types of activities that intermediaries can engage in (particularly the distinction between broadcasting and telecommunications, see Denton, 2014a; Karadeglija, 2015a). While Canadian federal policies have had a great deal in common with the liberalized regulatory approach of the United States (Birdsall, 2000), the Canadian state (principally through the CRTC and Cabinet) has been more willing to intervene through policies to promote competition and regulate relationships between incumbents and smaller competitors.

In 2017, amid rising protectionism and the collapse of international trade deals, any claim that we are living in a neoliberal era requires significant qualifications. While some are wondering how to characterize this (post-neoliberal?) world (Harvey & Morozov, 2016), I argue that Canadian telecom policy was never neoliberal to begin with, and remains fundamentally unchanged in recent years. Certainly, there have been many neoliberal arguments made to promote telecom policy since the 1980s, and for a time around 2006 these arguments seemed to become guiding principles of telecom policy. But the neoliberal policy guidance from this period (specifically, Government of Canada, 2006), which the CRTC still feels obliged to cite in its decisions, has little bearing on how Canadian telecom is actually regulated. As in many industries around the world, Canadian telecom governance has only partially reflected the neoliberal agenda. This has meant embracing liberalization, as a shift to commodification and market logic, while rejecting (or indefinitely delaying) deregulation, since the shift to markets has created a need for new regulatory regimes.

Regulatory capitalism and the economization of connectivity

In light of the previously-discussed weaknesses of the 'neoliberal revolution' as a description of contemporary governance, some alternate conceptualizations have been developed to explain the transformation that has taken place since the end of the 1970s. Among these, the 'regulatory state' (Majone, 1997) refers to a shift in emphasis away from governing through taxing and spending, and towards rule-making and market regulation. More recently, this has been incorporated into a theory of regulatory capitalism (Braithwaite, 2008; Levi-Faur, 2006), which combines aspects of neoliberalism (privatization and liberalization) and the regulatory state (regulating markets for the public good). Under regulatory capitalism, the shift is toward "more capitalism [and] more regulation" (Levi-Faur, 2006, p. 521), wherein "controls are achieved by the supreme command of the two regulators: the market and the state" (Levi-Faur, 2006, p. 497).[72] Rather than neoliberalism dismantling anything that opposes market logic, we

[72] Rather than the "retreat of the state" often identified in neoliberal analyses, authors mapping the contours of regulatory capitalism show how the role of the state has changed – with states becoming less involved in some areas (privatization of service provision) and expanding in other ways ("steering" the market through regulation, see Levi-Faur, 2006, p. 505). The specific path taken by Canada in this regard is unique, with some countries (like the US) opting for fewer wholesale obligations, and other countries (including some in Europe) pursuing a more radical approach known as "structural separation", in which the operator/provider of a network is banned from competing with the service providers who use the network (OECD, 2011). However, the fact that telecom

have the "regulatory capitalist reality of hybridity between the privatization of the public and publicization of the private" (Braithwaite, 2008, p. 8). In Canadian telecom, we see this in the expectation that the public good of connectivity should be provided as a commodity by private industry, but also as the various responsibilities imposed on private industry to serve the public good. Markets distribute connectivity as a good, but public policy tries to steer markets toward public ends (like a more equitable or competitive distribution).

While regulatory capitalism provides a more accurate conceptualization of the relationship between state power and private industry than the theory of the neoliberal transformation, it remains a broad generalization that can only serve as a starting point. The same methodological critique that is applied to neoliberalism is therefore also valid for regulatory capitalism: "Such broad concepts and visions may be useful at first, when certain changes need highlighting and outlining, but they become a hindrance once it becomes necessary to focus analysis to gain theoretical and political traction with specific developments" (O'Malley, 2016, p. vi). It is better to specify particular governmental techniques in play, such as increases, decreases or transformations in particular forms of regulation, rather than ascribing these to a governmental project as vast as neoliberalism or an order as diverse as regulatory capitalism. When we pay close attention to Canadian telecom regulation, it becomes clear that the logic of liberalization has itself shifted and been subject to dispute since the 1990s, with regular contests over the shape and extent of competition.

I will examine these specific governing techniques and logics in the following two chapters, but first there is one more broad generalization to cover that is related both to neoliberal

liberalization in Canada has resulted in more extensive regulation by a larger number of regulatory agencies (see Rideout, 2003, p. 147) is consistent with developments elsewhere in the world.

arguments and the reality of regulatory capitalism – what I characterize as the "economization" of connectivity (W. Brown, 2015). In Canada, regulatory liberalization may fundamentally be about opening new domains to market competition, but this has been accompanied by a tendency to value the economy above all else, and to approach the problems of connectivity primarily on economic terms. In this context, subjects are conceptualized primarily as market actors, whether these are competing intermediaries or individual consumers. This is demonstrated in the centrality that the CRTC and the federal government accord to the 'digital economy' (see CRTC, 2013c, 2015c, 2015e, 2016f; Dobby, 2016b), wherein the primary value of connectivity is not to enable citizenship, social relationships, or human flourishing, but for Canadians to "fully participate in the digital economy" (Government of Canada, 2016).[73]

This economization of connectivity is important because it means that certain justifications (the 'business case' for connectivity) and forms of knowledge (economic analysis) are privileged in Canadian telecom policy discussions and through the regulatory decisions of the CRTC.[74] But while other forms of rationality are often marginalized, they are not wholly excluded, and as seen in the following chapter, may even be significant drivers of particular connectivity projects.

ISPs in Canada today: Network topography and political economy

Today's internet still operates on the basis of some decades-old protocols and principles, but it is a far different creature in form and substance than the networks of the early 1990s. If we were to look farther back, to ARPANET and the 1970s (see Abbate, 1999; Hafner & Lyon, 1996;

[73] I am grateful to Tamara Shepherd for helping to crystallize this point.

[74] This was not a dramatic departure following liberalization, as even during the monopoly era, state-owned utilities were promoted on the basis of their "business-like management" (Armstrong & Nelles, 1986, p. 322).

Leiner et al., 2009), the link to today's ISP industry can be hard to recognize. Indeed, as previously discussed, it is more important to understand the early ISPs of the 1990s in the context of telecom liberalization, than as the technological culmination of packet-switching technologies that had developed over previous decades. While packet-switching was a technological innovation, today's internet is the product of specific public policies that shaped its commercialization.[75]

The first Canadian ISPs included publicly-funded academic networks, non-profits (such as FreeNets – see Chapter 2) and commercial organizations. There was considerable overlap between these categories, with partnerships between government and industry, commercial uses of academic networks, and links between academia and FreeNets (CA*net Institute, 2001; Hunt, 2014). These organizations had developed at the margins of public awareness in the early 1990s, but by the middle of the decade the World Wide Web had transformed the internet into a network with broader appeal and new commercial possibilities, forcing regulators to decide key questions of political economy. Even where these transformations happened in the absence of regulation, the choice not to exercise sovereign control became a public policy decision.

For example, some of the first Canadian ISPs depended on the "Centrex" digital line service offered by telcos to provide connectivity. Start-up costs and fees for use of the service were low, and numerous small IISPs (including FreeNets) competed with each other by utilizing

[75] Many accounts of the internet's development have attributed its success to an unregulated environment and a 'hands-off' attitude by the US government, combined with an independence from telecom monopolies. According to this narrative, the internet succeeded precisely because it was free from control by both government and the telecom incumbents. What is sometimes missing from such accounts is the extent to which the nascent personal computer and networking industries were protected from telecom incumbents by government regulation and anti-trust actions in the US. Active government intervention created the sorts of separations of roles and non-discrimination policies that are now known as "net neutrality" (Kushida, 2015). Limitations on ISP liability for copyright and "decency" (pornography, defamation), as well as a permissive privacy regime, also contributed to the global leadership of US internet industries (Chander, 2013).

telco infrastructure.[76] In 1995, IISPs appealed to the CRTC and the Competition Bureau when incumbent telcos withdrew the Centrex service, offered a replacement for a higher price, and entered the ISP market themselves (“ISPs Put the Boots to Telco,” n.d.; Winseck, 1998, pp. 297–298). By rejecting the IISPs’ appeal, regulators effectively decided what kinds of organizations were legitimate competitors in the new market, and what power these incumbent intermediaries would have over their dependents (see Chapter 3).

With incumbent telcos and cablecos now operating as ISPs, many smaller competitors were absorbed or went out of business. Through the latter half of the 1990s and into the early 2000s, a shrinking number of large ISPs came to control more of the market (Winseck, 2015b). Even as the CRTC mandated new forms of wholesale access to incumbent infrastructure in order to promote competition from new entrants (see Chapter 3), regulators showed a permissive attitude towards this growing concentration. Consolidation throughout the telecom industry was not just a matter of larger companies swallowing smaller ones, but also included sizable mergers, such as the one that created TELUS out of B.C. and Alberta's telco incumbents in 1999. By 2004 (when MTS moved to purchase Allstream), one telecom consultant noted that there wasn't much left to consolidate, with the exception of municipally-owned telcos such as those scattered across Ontario, or the power companies that possessed telecom infrastructure (Wire Report, 2004). But the trend towards the consolidation of giant firms has continued, with recurring efforts towards merging Bell and TELUS (Marowits, 2007; Nowak, 2009),[77] and Bell's purchase of MTS

[76] At one point, the B.C. internet association represented a hundred and fifty ISPs (M. Hrybyk, personal communication, May 4, 2016). Winseck (1998, pp. 296–297) estimates between 15 and 20 ISPs existed in major cities like Vancouver (see M. Wilson, 1997), and half a dozen in mid-sized cities such as Windsor.

[77] While Bell and TELUS have remained distinct corporate entities, they do share one another's wireless facilities (Bell using TELUS facilities in western Canada and TELUS using Bell's in the east) – something that competitors have often pointed out in debates over wireless competition (see CPAC, 2012, 2013a).

(Jackson, 2017a) testing regulators' limits of acceptable competition.

Internet connectivity in Canada today is therefore dominated by telco and cableco incumbents,[78] which are currently transitioning to fibre-optic access networks (using fibre for the 'last mile') where there is a business case.[79] Incumbents do compete with one another, but not all incumbents compete all of the time, since many are satisfied serving their established territories and see no value in duplicating facilities where another incumbent is present. Hundreds of IISPs of various sizes are scattered across the country,[80] competing with incumbents in urban areas (where multiple ISPs often provide access) or focusing on less-profitable rural areas where residents lack choices. IISPs have maintained or expanded their market share against the incumbents (Winseck, 2015b), but their continued viability is enabled by the CRTC's mandated access regime. While this regime affords IISPs a measure of protection against larger competitors, IISPs remain dependent on the incumbents they typically rely upon for either wholesale or last-mile access (see Chapter 3). This dependence is tied to control over the internet's topography. The internet's critical bottlenecks are the fibre-optic routes to and from major internet exchanges in Vancouver, Toronto and U.S. cities. If an ISP can find a path for its traffic to one of these IXPs, it can negotiate directly with major global players: international long-distance networks and services such as Google, Facebook and Netflix. While incumbents control paths to multiple internet exchanges, IISPs typically lack such direct access. This means that IISPs rely on incumbents to connect to the broader internet, giving incumbents tremendous leverage, and it is the CRTC's mission to keep this 'market power' in check.

[78] In 2015, the five largest companies (Bell, MTS/Allstream, Rogers, Shaw, TELUS) accounted for 84% of total market revenues (CRTC, 2015f, p. 151).

[79] For instance, in new housing developments or where the cost of a network upgrade would be well-compensated by broadband subscriptions.

[80] The CRTC reports that there were approximately 525 ISPs across the country in 2015 (CRTC, 2015f, p. 202).

While the CRTC adjudicates disputes over rates and access, an important stake in these debates is the very kind of governing rationality at play in telecom policy. For example, recent CRTC reviews of wholesale and basic services (CRTC, 2015c, and 2015e respectively) were not just contests over what the networks of the future would look like (where these networks would extend, using what technologies, and who would control or use them), but also what the underlying objectives, justifications, and methods of telecom policy should be. Many have pointed to the *Telecommunications Act* (Government of Canada, 1993) or the 2006 policy direction (Government of Canada, 2006) as specifying these policy objectives and the means to achieve them, but portions of these texts have been cited in different ways to justify competing visions of telecom policy and competing governmental techniques.

With a perspective informed by governmentality and nodal governance, my focus will not be on foundational documents, but rather on the specific techniques, rationalities, and relationships that are relevant for ISPs on a day-to-day basis. While previous analyses have focused on the transformations of the 1990s, characterized as deregulation (Wilson, 2000), neo-liberalism (Rideout, 2003), or convergence (Winseck, 1998), this work is situated in a political economy that has largely stabilized under the regulatory capitalism of the internet era. What exists today was not the end-state imagined when major policy shifts were initiated nearly thirty years ago, and rather than a market equilibrium, its stability is maintained through regulation. Liberalization is a process that is always incomplete, and in Canadian telecom it has become a mode of governance that is continually being recalibrated by a number of state agencies. The specific policies being pursued through intermediaries remain open to revision and expansion, but what has steadied is a political economy dominated by incumbents and a regulatory state that both legitimates and limits the power of these corporate giants. The CRTC is the most visible state actor that cultivates and elevates the economic forces that telecom incumbents represent (the economization of connectivity), while restraining incumbents through its claim to sovereign authority.

Under regulatory capitalism, society is governed by an alignment of private market actors and the public interest, but this does not specify what the public interest is, or the regulatory techniques to achieve it. The following chapter addresses what happens when connectivity itself is conceived of as a ‘public good’, and the variety of techniques for improving connectivity where competition and market forces are deemed inadequate.

Chapter 2: The public pursuit of connectivity

The acknowledgement of broadband being vital to economic, social, democratic and cultural success of individuals and collectivities is a given. However, this only brings us so far. Three other questions must be asked.
First, where are the gaps to access to connectivity?...
The second question is, given those gaps, what are the best strategies in order to close or eliminate them? And finally, who is in the best position to implement those strategies?...
-CRTC Chairman Jean-Pierre Blais, April 18, 2016 (CRTC, 2016a)

Many of the public policy objectives at the heart of internet governance discussions have been deeply controversial. For instance, should ISPs do more to assist law enforcement or copyright owners? Should ISPs practice "net neutrality", by not discriminating amongst traffic? Should incumbent ISPs be required to treat smaller competitors as wholesale customers? Underlying these debates is the shared assumption that connectivity is, in and of itself, a good thing. The internet's policy consensus, or the assumption upon which other governing rationalities are based, is that the greater the number of people who are connected, the faster their connections, the better. The public policy goal of improving connectivity is not controversial; it is the question how to achieve better connectivity that has generated intense debate. This chapter will consider what happens when connectivity is treated as a public policy objective, and ISPs are the instruments to achieve it.

My argument is that efforts to provide connectivity as a public good, which date to the very origins of the internet as a public network, create persistent tensions and role conflicts around ISPs' expectations following telecom liberalization. Telecom networks share many of the characteristics of other kinds of traditionally public infrastructure, such as transportation networks and utilities. But because of the expectations applied to public organizations and private intermediaries, role conflicts result when commercial intermediaries provide connectivity as a public good, and when public organizations operate in a role similar to that played by commercial intermediaries. Since telecom liberalization, the governing rationality has required intermediaries to compete with one another, and for connectivity to be treated as a private good allocated through market forces. This means that there has been a reluctance to pursue connectivity as a public policy objective through dedicated public institutions, and those public organizations that play the role of intermediaries must carefully delimit themselves so as not to compete with private industry. Private industry, on the other hand, has repeatedly been enlisted toward public policy ends, but this has been accomplished by trying to make public policy profitable, either by designing incentives for improving connectivity or simply paying private industry to build and operate infrastructure. The track record for such projects has been mixed in Canada, and the contradictions of profit-seeking actors serving the public good are manifest in these outcomes. However, role conflicts also often grant considerable discretion to the intermediaries that must resolve them, as seen in the range of approaches that have been taken to resolving the problem of connectivity.

Pursuing connectivity

Public policy interventions have typically tried to address gaps and inequalities in connectivity, rather than improving connectivity for all Canadians. While the internet may stretch around the globe, connectivity remains geographically uneven, often following the lines of legacy infrastructure.[81] In some ways, these inequalities deepened in the 1990s, since the internet originally operated through telephone infrastructure, but is now also carried over the cable video

[81] This includes the transportation infrastructure. Just as early telephone lines were closely tied to railway infrastructure (Winseck, 1995), today's internet cables also follow roadways and railways, making the owners of these transportation networks crucial partners in many broadband projects.

network, or more exclusive fibre-optic deployments. In Canada, as with many other countries, telephone infrastructure was extended to individuals across the nation under a mandate of universal service. Cable (coaxial) infrastructure was accessible throughout urban areas (and offered generally better internet performance), but had limited reach in rural Canada. Both networks relied on fibre-optic backbones, and these have recently been extended to homes and businesses, but only in select areas. In short, access to the internet has and continues to be limited by access to its infrastructure, and this means that for many Canadians, connectivity remains a problem.

Since the 1990s, successive federal governments have committed to extending and improving connectivity in various ways. Provinces have pursued their own broadband programs, and some municipalities have also taken steps to manage internet infrastructure for public benefit. Numerous private ISPs have applied for government support or competed for contracts to build networks where market forces have failed to deliver. Some not-for-profit and charity organizations have also worked to address gaps in access. Finally, since internet connectivity is increasingly a prerequisite for other services or kinds of social participation, there are recurrent calls to classify broadband as a government-mandated "basic service" (Karadeglija, 2014c), to provide it as an "essential utility" (Alberta Economic Development Authority, 2010), or to recognize and govern the digital domain as a "commons" (Mueller, 2012; Telecommunities Canada & Industry Canada, 1997). In other words, connectivity is highly valued and recognized as having numerous public benefits, but approaches to improving connectivity have varied.

One view, more fully explored in the following chapter, is that connectivity is best pursued through private actors operating in a competitive market. But this rationality is frequently challenged by circumstances that might be characterized as 'market failure'. The most evident example of market failure has been in the provision of rural broadband, an issue which closely echoes the debates over rural telephone service in the twentieth century (Babe, 1990; Rens, 2001; Winseck, 1995). Connectivity is widely recognized as lacking in many rural areas, since companies have been reluctant to invest in rural broadband where the "business case" is weak (Rajabiun & Middleton, 2013, p. 7). However, this is not the only instance in which market-based solutions to society's 'connectivity problems' have been deemed insufficient or inapplicable.

While access to high-speed and affordable internet is a problem for much of rural Canada, even urban populations face connectivity challenges, and there are broad inequalities in how wealthy and marginalized populations make use of technology in their daily lives (Crang, Crosbie, & Graham, 2006). As scholarship in the field of community informatics has repeatedly emphasized, merely providing internet access is a partial solution to the 'digital divide' (Gurstein, 2003; Longford, Clement, Gurstein, & Shade, 2012, pp. 15–17; Rideout & Reddick, 2005).[82] Individuals need the skills to use tools and services effectively, and a level of understanding to see the possibilities that internet technologies enable. Improving connectivity is a straightforward objective when this is defined as connecting more devices to the network at higher speeds. The goal of connecting people (as internet users who are capable of exercising agency through technology) is a more complicated public policy objective that requires more than a technical solution. It makes little sense to say someone is connected to the internet when they are unable to effectively use the computer they depend on as an interface, or have difficulty

[82] This criticism has also been reflected in much of the scholarship on the digital divide since the late 1990s, which has emphasized skills and usage over physical access (van Dijk, 2006).

navigating a web browser. Many programs dedicated to furthering connectivity have neglected this aspect, or simply assumed that these human capabilities (the knowledge and skills to make effective use of the internet) exist in the populations they are trying to reach.[83] However, people can face a host of disadvantages in accessing online services irrespective of the speed of their internet connection.[84]

The telecom industry is not in the business of evenly distributing connectivity throughout society, and has generally failed to address the need for a broader, socio-technical approach to connectivity. Commercial ISPs are interested in gaining and retaining subscribers where it is profitable to do so, and see less value in helping these subscribers use the internet more effectively to meet their goals.[85] Connectivity might be a means to various social ends, but private industry is quite understandably focused on the end-goal of profitability.[86] As a

[83] There have been public policies in Canada that have sought to improve digital literacy skills, but efforts to improve connectivity have typically had a narrow, technical focus (see Rideout & Reddick, 2005). The CRTC recently “acknowledge[d] that a gap in digital literacy skills is a factor that can contribute to limiting consumers’ ability to participate in the digital economy and society”, but decided that “responsibility for the issue of digital literacy is not within the Commission’s core mandate” (CRTC, 2016f, para. 245). In the same decision, the CRTC recognized the gaps in affordability that act as barriers to connectivity for some populations, but argued this was best addressed by “foster[ing] a competitive marketplace” (CRTC, 2016f, para. 196). Meanwhile, the most recent federal public policy in the US to improve connectivity (ConnectHome), included both an effort to target low-income populations and a digital literacy component (Zezima, 2015).

[84] Clement and Shade (2000) have developed the model of the “access rainbow” to demonstrate the many facets or “layers” that can be required for access to network services. These go beyond expanding the telecom infrastructure that tends to be the focus of programs to improve connectivity, and can include affordable personal devices (or access to public terminals), software, and digital literacy (van Dijk, 2006).

[85] In the 2016 basic services review, telecom companies “indicated that they are not well-equipped to address digital literacy, and that this issue would best be addressed by governments” (CRTC, 2016f, para. 244). The most significant initiative through which incumbent ISPs (specifically Shaw, Rogers, TELUS, Bell) promote elements of effective use (Gurstein, 2003) is through their support of MediaSmarts, an organization devoted to promoting digital and media literacy in Canada, by helping “children and teens develop the critical thinking skills they need for interacting with the media they love” (MediaSmarts, n.d.). Incumbents acknowledge the problems of digital literacy (see Goodyear, 2016) and low-income access, but they also use these socio-economic gaps as a way of arguing that network access is not a problem and that government should not try to extend networks through regulation. In 2011, Michael Hennessy from TELUS stated that “the real barriers are no longer infrastructure investment but digital literacy and low income". Therefore, public investment in broadband infrastructure “is neither necessary nor in the public interest" because “those networks are already built and just keep getting better" (CPAC, 2011).

[86] In recent years there have been some exceptional cases of ISPs addressing inequality through dedicated

consequence, commercial ISPs are sometimes governed to serve the public policy objective of improved connectivity, or this role is played by public institutions. However, in both cases some degree of role conflict almost invariably results.

This chapter will review several types of public connectivity initiatives, namely publicly-funded networks and ISPs that are actively engaged in using connectivity as a means to meet larger social objectives. The range of approaches and organizational forms used to address the problem of connectivity in Canada has been remarkable, and this chapter will include an explanation of some of the different configurations of public and private institutions that have come together towards this end. The following chapter will analyze the pursuit of competition as the dominant expectation for intermediaries under regulatory capitalism, including how this expectation applies to publicly-funded networks, but first I must explain what the idea of connectivity as a public good entails, and the role of public or not-for-profit institutions in enabling connectivity.

Connectivity as a public good

What constitutes a public good is by no means self-evident. Economists have proposed different sets of criteria for defining public goods since the 1950s (Milleron, 1972, pp. 419–425), which specify whether something counts as a public good on the basis of inherent characteristics or the good's relationship to markets.[87] Connectivity, whether defined simply as a material

programs for the poor. Rogers offers discounted internet to low-income households in Toronto (in collaboration with other companies providing affordable hardware and technical support, see Monsebraaten, 2013), and TELUS (Jackson, 2016a; TELUS, 2016b) is now providing affordable connectivity to low-income single-parent families in B.C. and Alberta.

[87] Economists generally recognize public goods as being non-excludable and non-rivalrous in consumption (see Bodnar, 2007; Milleron, 1972). This means individuals cannot be excluded from consumption, and use or consumption by one individual does not reduce the ability of others to use or consume the resource. The internet

connection to the internet, or more broadly as the ability to make use of that connection,[88] might indeed qualify as a sort of public good under these formal definitions (see Fulk, Flanagin, Kalman, Monge, & Ryan, 1996), but it is not an ideal example.[89] This being said, public goods are increasingly being provided by non-state actors (especially since the 1980s, see Kaul & Mendoza, 2003). Public good theory provides ample justification for various kinds of interventions to maximize the benefits of connectivity (Gómez-Barroso & Feijóo, 2010), which need not extend to state agencies providing internet access. Instead, governments around the world have championed a variety of public policies to promote connectivity, alongside a rationality in which private industry takes the lead in building and operating infrastructure. Some of the most common interventions are those that allocate public funds to geographic areas where private initiatives are expected to arrive late or not at all (Gómez-Barroso & Feijóo, 2010, pp. 490–492).

For my analysis, the question of whether broadband internet access is inherently a public good is less important than the ways it has been defined as such. In other words, public goods are classified and governed through a political process (see Kaul & Mendoza, 2003; Stone, 1991, Chapter 2), so that what counts as a public good and the consequence of this classification is itself a matter of public policy. These questions have surfaced in Canada at all levels of government, including CRTC discussions about whether all Canadians should have access to broadband,[90] provincial and regional efforts to extend connectivity by funding new networks, and

now arguably qualifies as non-excludable, in the sense that all members of Canadian society require access to it in some fashion. Usage is rivalrous in the sense that too much usage causes network congestion, but over-use can be a problem for other widely-recognized public goods (water, power).

[88] What Fulk et al. (1996) distinguish as physical and social connectivity.

[89] It might instead be considered a “mixed” or “merit good” (Gómez-Barroso & Feijóo, 2010, p. 488).

[90] Most recently, in the 2016 review of the CRTC's basic service objective (CRTC, 2016f).

municipalities' roles in managing broadband as public infrastructure.[91] Proponents of these efforts to expand connectivity may not explicitly invoke the public good as a rationale,[92] but they recognize a broad public benefit derived from internet access and see a role for public agencies (or public funding), rather than entrusting the distribution of this good entirely to private markets. Typically, this means aligning private ISPs with the goal of improved or more equitable connectivity, whether through government-imposed requirements or through government contracts. More rarely, public bodies (namely, municipal governments) have undertaken the task of building and operating entire networks. However, this approach contradicts the prevailing liberal ethos that networks should be owned and operated by private companies, and is typically criticized as government interference in the market. I will also consider the descendants of the publicly-funded research and education networks that preceded the commercial internet, some of which are finding innovative new roles beyond the business scope of private ISPs.

In instances where ISPs provide connectivity as a public good, connectivity is rarely promoted as an end in itself. Instead, broadband is understood to be an enabler towards other public policy objectives (Joselyn, 2013, p. 90). Particularly in rural regions suffering various forms of decline or inequality as compared with urban Canada, broadband is promoted as a way to attract desirable elements to communities (including new residents and businesses) and to overcome various challenges posed by distance and isolation (Agriculture and Rural Development, 2009; Castlegar News, 2014; Government of Alberta, Axia Netmedia, & Bell Canada, n.d.; OICRD, 2011; Rossland Broadband Initiative, n.d.; Stoesser, 2015).

[91] (Digital Futures Symposium transcript, November 14, 2013; S. McLeod, personal communication, March 14, 2014; Wolfe, Vennard, & Mitchell, 2014, pp. 5–6). There are related arguments about the status of rights-of-ways, see note 177 below.

[92] Explicit references to the public good are comparatively rare in Canadian telecom policy discussions and the formal regulatory process (see Rajabiun & Middleton, 2015, p. 51).

While benefits as diverse as greater community solidarity and democratic participation have been presented to justify some of these efforts, in the current Canadian milieu, the value of broadband tends to be rationalized in economic terms (much the same is true in the US, see C. Mitchell, 2014). New networks are 'sold' to potential backers as a way of improving competitiveness, enabling local entrepreneurship, and attracting new businesses.[93] A particularly effective argument in favor of municipal networks is the promise to reduce municipal spending on contracts with private ISPs, possibly even generating municipal revenues through publicly-owned infrastructure.[94] Economic arguments tend to carry the day, and are far less controversial in Canada than notions of a 'universal right' to internet access or the idea that broadband should be regulated as a utility. These alternate discourses have existed since the earliest days of the public internet in Canada (as evidenced by the FreeNet movement described later in this chapter), and a number of actors still promote the argument that internet infrastructure should be publicly-owned, or that market-forces should be limited to competition in online services.[95] But these remain marginal voices against dominant support for the broad outlines of the liberalized status quo, wherein private ISPs are expected to improve connectivity through the pursuit of profit. Arguments for alternate approaches, such as publicly-funded networks, are typically expected to justify themselves as exceptions to this prevailing view. The most uncontroversial of

[93] (Digital Futures Symposium transcript, November 14, 2013; Dobson & Graham, 2016). It should be noted that the economic benefits of extending and bettering connectivity are far from certain. Studies have found measurable improvements in a number of indicators following broadband deployment (see Rajabiun & Middleton, 2013, pp. 7–8), but there is no guarantee that the presence of high-speed internet will convince businesses to relocate or attract new immigrants. Lofty expectations have often been created to justify broadband investment, which when left unmet, can create additional problems (Tapia & Ortiz, 2008a). Numerous publicly-funded networks that have failed to deliver on such promises and been bought out by an incumbent ISP (see note 149 below).

[94] (Digital Futures Symposium transcript, November 14, 2013; R. Adams, personal communication, November 8, 2013; Wire Report, 2000b).

[95] These are variants of the service-based competition argument explored more fully in the following chapter.

these justifications are that publicly-funded networks can serve the needs of public institutions, or that public investment is warranted where it can ultimately help private industry to thrive. These two justifications have combined in interesting ways to legitimate to continued existence of Canada's research and educational networks, described below.

Publicly-funded networks for research, education and entrepreneurial innovation

The internet's roots, in both the US and Canada, lie in publicly-funded networks for the purposes of research and education (see CA*net Institute, 2001; Shade, 1994). FreeNets and commercial uses followed the academic networking of the 1980s, and while most of Canada's internet infrastructure is now privately managed, tens of thousands of kilometers are still leased or owned by public institutions to serve a public mandate. Setting aside those networks run to meet internal government needs (such as the federally-contracted SCNet, or municipal networks used simply to interconnect government buildings) there are numerous networks of various size across the country that use public funding to provide connectivity in the public interest, the oldest of which are the research and education networks (RENs) that extend through provinces and territories.

These twelve provincial and territorial RENs[96] are interconnected through a national "long-haul" internet backbone, originally formed in 1990 as CA*net (CA*net Institute, 2001; Shade, 1994). The core function served by RENs is to provide connectivity to research and educational institutions, but the rationale for their existence often includes an economic argument. While purely academic networking initiatives were carried out in Canada prior to CA*net, the early 1990s saw a growing number of tensions and overlaps between the needs of

[96] These are knowns as ORANs - Optical Regional Advanced Networks.

universities, private users, businesses, and the telecom industry (CA*net Institute, 2001). CANARIE, which now operates the national REN backbone (NREN), was established with an explicit mandate to support industry and the "information-based economy" (Silva & Cartwright, 1992).[97] Incumbent telcos have been instrumental in the backbone's operation and are represented as stakeholders on CANARIE's board of directors. This has previously resulted in conflicts over the organization's mission, as when CANARIE's promotion of community fibre networks created a backlash from incumbent board members who feared a loss of business (Wire Report, 2000b). More recently, the infrastructure of RENs has been actively promoted for business innovation and entrepreneurship. CANARIE's DAIR program "leverages Canada's investment in the CANARIE national backbone... to accelerate product development and improve the market competitiveness of small and medium-sized Canadian companies" (CANARIE, n.d.). DAIR provides free cloud computing resources to companies developing new products or seeking to bring them to market.

One of CANARIE's provincial partners and a participant in the DAIR program is Cybera, which operates Alberta's REN (known as CyberaNet). This not-for-profit organization is funded by a grant from the province's Ministry of Innovation and Advanced Education and membership fees from its members.[98] Cybera's core mandate is to provide connectivity through CyberaNet to

[97] CANARIE rose in importance with the commercialization of the NREN backbone in 1997, when CA*net was dissolved as an organization and its assets were sold to Bell (CA*net Institute, 2001). As Bill St. Arnaud, formerly Chief Research Officer at CANARIE (employed between 1993 and 2010), stated: "CANARIE's mandate from day 1 was always industry development. That is why CANARIE was always funded by Industry Canada and not the research councils. In the early days CANARIE did not even operate a R&E network. Its core function has remained unchanged. Externally it might have appeared that its core function was to operate an R&E network. Internally one of CANARIE's ongoing challenges was always to see how operation of a R&E network fitted with its core mandate of private sector innovation" (personal communication, October 18, 2014).

[98] Cybera also receives some project-based funding from CANARIE (Cybera, 2014a, p. 2).

its members, which are primarily public-sector educational institutions.[99] However, research, education, technological innovation and "enterprise" are closely linked government priorities in Alberta.[100] In 2010 Cybera's Board of Directors hired a new entrepreneurial-minded CEO (Cybera, n.d.-b), interested both in business promotion and the public good (including the commercialization of new technologies and publicly-funded research). Cybera subsequently developed or participated in a variety of "above the network" projects such as shared cloud computing resources and software development, and now describes its mission as "overseeing the development of Alberta's cyber-infrastructure" (Cybera, n.d.-a).[101]

Cybera has therefore evolved into a unique sort of intermediary, concerned both with basic connectivity through CyberaNet, and using this public network to power "research and innovation projects", such as aiding entrepreneurs in the early stages of "bringing technology to market" (Cybera, 2013, pp. 4–5). The organization's broad, quasi-public scope and mandate has resulted in some interesting approaches to its core mission of providing internet connectivity to its members, and broader discretionary efforts to promote connectivity in the province. These have included participating in the development of an internet exchange in Calgary to strengthen local connectivity,[102] and finding ways to lower the cost of internet for its members by aggregating their demand to negotiate better wholesale rates, or peering with some of the most

[99] Chiefly schools and post-secondary institutions, but also not-for-profit organizations and "pre-commercial enterprises" (http://www.cybera.ca/membership/membership-structure/).

[100] The Ministry of Innovation and Advanced Education was previously named Enterprise and Advanced Education, and prior to that, Advanced Education and Technology.

[101] (M. Hampel, M. L. Lee, & D. Chan, personal communication, September 26, 2013; R. Winsor, personal communication, June 16, 2014).

[102] An internet exchange is a location where ISPs can exchange traffic, or connect to other providers such as CDNs. Canada has for a long time suffered from a notable lack of IXPs, which limited the options for smaller ISPs and kept them dependent on local incumbents. The development of Calgary's internet exchange was a particularly contentious process (de Raadt, 2013a, 2013b; R. Winsor, personal communication, June 16, 2014), with a fracture that briefly resulted in two parallel exchanges (YYCIX and ABIX, the latter of which was supported by Cybera). Only YYCIX proved viable, and Cybera joined the exchange in December 2014 as a peer (Cybera, 2014c).

popular content providers (Cybera, n.d.-a). Cybera's facilitation of “public cloud computing” (Cybera, 2015a) echoes the 1970s dream of a Canadian computer utility (Mussio, 2001, Chapter 7), albeit for a more limited range of users. While the organization has emphasized that it does not “work where commercial companies are offering competitive services” (Cybera, 2013, p. 5), this does not preclude it from offering cheaper bandwidth to schools connected to incumbents or the SuperNet.[103] Cybera has also taken positions that conflict with telecom incumbents on some key issues, arguing for “internet as a right” through greater wholesale access to incumbents' fibre infrastructure and for a fundamental shift away from “facilities-based competition” to “service-based competition” (Cybera, 2014b), as discussed in the following chapter. Cybera also argues there is “a strong case to be made” for municipal ownership of telecom infrastructure to address urban-rural inequalities, albeit with private companies maintaining and providing services over such networks (Cybera, 2015b, p. 12). This makes the organization unique in Canada, promoting improved connectivity throughout society as a public policy objective, while other regional RENs remain largely focused on their core mandate of connecting research and educational institutions.[104] However, other kinds of intermediaries also work towards the public policy objective of reducing inequalities in connectivity.

[103] CyberaNet does depend on SuperNet for much of its reach, particularly in the last-mile, but the two are separate networks (customers with a direct or leased connection to CyberaNet can skip SuperNet altogether). By offering schools lower rates for internet connectivity through its connections to major internet exchanges, Cybera has boasted that it has “spurred the major carriers to compete for the internet buy of Alberta’s educational institutions, and in so doing has dropped rates from hundreds of dollars to around ten per Mbps” (Cybera, 2014a, p. 5)

[104] The exception here is BCNET, and the organization's active efforts to develop internet exchanges in that province (Hay, 2013; M. Hrybyk, personal communication, May 4, 2016; C. Lee, personal communication, November 8, 2013).

Bridging the digital divide: ISPs as instruments of equitable connectivity

As a growing number of services now presume internet access, disparities in connectivity have been brought into starker relief. The undeniable fact is that with every passing year, connectivity is required for a growing number of social interactions and relationships. It becomes harder to opt out of these digitally-mediated interactions without losing access to important services and opportunities. The internet is now society's connective tissue, and poorly-connected segments seem destined to atrophy. The more essential connectivity becomes, the less need there is to justify its benefits for everyday life,[105] since the consequences of lacking access to broadband become readily evident. Rather, the key points of debate come to hinge on the question of how to best provide connectivity to everyone, with all levels of government retaining considerable discretion in this regard. In Canada, the governing rationality of regulatory liberalization since the 1990s has argued that internet provision should be left to a healthy, competitive private industry. But many Canadians have been poorly served by this market-based approach, leading to alternate models of connectivity such as those discussed in this chapter.

Inequalities in connectivity have often been characterized as a "digital divide" between privileged and disadvantaged groups. In academic elaborations of this concept, authors have identified disparities in connectivity between rich and poor, old and young, urban and rural, men and women, as well as different racial and ethnic groups (Howard, Busch, & Sheets, 2010; van

[105] The consensus around the importance of connectivity was best demonstrated by CRTC Chairman Blais' unprecedented decision to interrupt the 2016 basic services hearing to state the "self-evident" truth that "broadband is vital... to economic, social, democratic and cultural success of individuals and collectivities" (CRTC, 2016a). However, there is still a debate about whether the benefits of broadband increase as connectivity improves beyond a certain level. For example, "gigabit networks" such as the one built in Olds, Alberta, offer vastly more bandwidth than residential subscribers typically require today, are constrained by the speed of the rest of the internet (Farivar, 2012), and are justified in large part by future needs. Some incumbents have argued that consumer demand simply does not exist for speeds beyond what is available to most Canadians (CRTC, 2014f).

Dijk, 2006). In short, all of the traditionally-recognized social inequalities are reflected in unequal access to the internet, or in unequal abilities to make "effective use" (Gurstein, 2003) of ICTs. Many of the networks and organizations discussed in this chapter operate under the rationale of bridging these digital divides. These ISPs are either the outcomes or instruments of policies that redistribute the kinds of capital necessary for connectivity (see Selwyn, 2004). In many cases, public sources of funds (tax revenues, infrastructure loans) are directed to building out networks in areas where internet penetration has been deficient. However, before discussing these networks, I will consider FreeNets as an alternate model quite different from the top-down implementation of public policy. The FreeNet movement of the mid-1990s provides some of the best examples of ISPs providing connectivity towards the public good,[106] under an equitable and redistributive governmental rationale that stands in stark contrast with today's dominant (commercial and public) approaches.

FreeNets: Distributing connectivity as a public good

The FreeNet[107] movement was an extraordinary phenomenon that (alongside RENs) helped define the early years of the internet in Canada.[108] Eventually, ideas of free access and community networking were overtaken by the business models of the commercial ISPs that remain dominant today. However, in the mid-1990s the future of the public internet was still

[106] One of the most explicit articulations of public good principles to internet access in Canada occurred as a result of the Vancouver FreeNet Association's application for charitable status. While the application was initially denied, Justice Hugessen's judgment at the Federal Court of Appeal recognized the "free exchange of information amongst members of society" as a public good, and likened the internet to previous systems of communication such as public roads (Bodnar, 2007; *Vancouver Regional FreeNet Assn. v. M.N.R.*, 1996).

[107] Also known as Free-Net, not to be confused with Freenet (which is a peer-to-peer platform designed to be resistant to censorship).

[108] While concentrated in North America (as with the early internet), FreeNets were organized around the world in the 1990s and early 2000s (P. Scott, 2001) – very few of these networks remain today.

wide open, with vast but largely untapped possibilities, and so it seemed quite reasonable that connectivity should be conceived and provided as a public good. Groups of individuals scattered across the country, learning from one another, pursued an egalitarian and community-minded vision of digital networking. The details of these visions varied from case to case, and access to the broader internet was typically only one of the services provided by these organizations. But in general, the idea was that connectivity should be available free-of-charge, or that cost should not be an obstacle for anyone wishing to be connected. FreeNets (sometimes identified under the broader category of "community networks") depended on volunteer labor, corporate donations, and government assistance. Instead of subscribers, FreeNets had members, some of whom donated a regular amount and thereby subsidized those with free access. In addition to making basic connectivity affordable to all, these not-for-profits[109] developed online information that was locally-specific, coordinated volunteer assistance, and promoted the use of connectivity in the service of lofty social values, such as community development,[110] democratic participation, and "digital inclusion" (Avis, 1995, pp. 81–88; G. Graham, 2011; Taylor, 1993).

The earliest FreeNets preceded the commercial internet; the first was established in 1986 in Cleveland, and 1992 saw the birth of the Victoria Free-Net Association as well as Ottawa's National Capital FreeNet (NCF) (Servon, 2002, pp. 53–54; Shade, 1994; Victoria Free-Net Association, n.d.). It is difficult to say how many such networks existed across Canada at the movement's peak, but around forty are listed on a webpage archived in 2001 (P. Scott, 2001).[111]

[109] As an exception, Vancouver FreeNet was ultimately successful in being recognized as a charitable organization (see *Vancouver Regional FreeNet Assn. v. M.N.R.*, 1996).

[110] Including the work of Telecommunities Canada (see note 112 below) in advocating for local control over broadband networks as a way to promote local ("community") autonomy (G. Graham, 2011; personal communication, September 26, 2015).

[111] Bodnar (2007) counts 26 in in Canada in 1995, with 67 "in various stages of development". However, by 2007 this number had been reduced to approximately six.

Today, we might only be able to count three or four operational descendants of those early FreeNets (most notably in Vancouver and Ottawa). These survivors are a far cry from the initial optimism and revolutionary potential of the FreeNet movement, which was never able to emerge from the dial-up era once incumbent ISPs made the shift to broadband. For Bodnar, the inability of so many of these networks to remain viable into the 2000s indicated that "the once-common objective of providing free or low-cost Internet access and community-based resources in the service of public access... [was] no longer as straight forward as it once seemed" (Bodnar, 2007). And yet, some of the core problems that FreeNets tried to solve – inequalities in connectivity, effective use, and the need for community development are no less relevant today. But our capacity to 'think otherwise' about the future of the internet seems to have narrowed. The mid-1990s were a crossroads, and the path then taken onto the privately-managed information highway has precluded further consideration of alternatives.

In retrospect, the birth and apex of the FreeNet movement occurred during a brief window in the internet's development, specifically between 1993 and 1994.[112] This window saw

[112] In August 1993 the *International Freenet Conference* was held in Ottawa, sponsored by NCF and the federal Department of Industry and Science (NCF, n.d.-b). It included sessions on how to start and sustain FreeNets, and was repeated the following year as the *Canadian Community Networks Conference* (NCF, n.d.-a), which was also the founding meeting of Telecommunities Canada. This organization would go on to be an umbrella-group and champion of various kinds of community networks, such as community access points under the federal government's CAP program (Longford, Clement, Gurstein, & Shade, 2012, pp. 8–12). According to Garth Graham (personal communication, September 27, 2015), what may have been the organization's highest achievement came in 1997, when the organization partnered with Industry Canada and released a *Framework for Co-Operation...to enhance the ability of Canadian communities to utilize electronic public space*. This remarkable document shows that even at this later point in the internet's development, Industry Canada was willing to acknowledge a vision of the future in which connectivity would promote local autonomy, and one in which the "community network extends the idea of community into a shared electronic public space, a new not-for-profit transaction space", also described as a "public commons" (Telecommunities Canada & Industry Canada, 1997). According to Graham, this official recognition of community networking was an attempt to neutralize the political threat from Telecommunities Canada, which in the end, "never had the energy/resources to act on [its] part of implementation" (personal communication, September 26 & 27, 2015). After 1997, it was clear that the federal government's public policy approach to connectivity favored the commercial rationality of incumbents over such lofty social values.

the internet outgrow its publicly-funded incubator and extend into public access, but only lasted until the telecom industry stepped in with its own business plan. One of the founders of the NCF (Jay Weston), remarked that if the organization had been established in 1995, “it is unlikely that the telecommunication industry and various governments would have been so unconcerned, or benignly neglectful, of what the freenet implied” (Avis, 1995, p. 86). Also in 1995, the internet's US backbone switched from a publicly-funded network (NSFNET) to several interconnected commercial backbones, effectively privatizing the internet. The World Wide Web emerged, and FreeNets such as NCF had to decide whether (and how) to provide access to it (Hunt, 2014, p. 32; “National Capital FreeNet,” 2014). Private ISPs were founded across the country to serve the growing demand, and by 1996 Canadian telecom incumbents had entered the market and become dominant ISPs.[113] At that point, FreeNets were no longer charting the future of Canada's internet, but simply trying to adapt to the changing environment.

FreeNets offered a competing vision for intermediaries’ governing rationality; opening internet access to all, supporting “effective use” (Gurstein, 2003), and directing group energies toward noble social objectives. They were able to ride the first wave of public interest in the internet (see Elder, 2002), and while they seemed to be an open-ended instrument for the public good in a networked era, a lack of stable funding and the rapidly-changing environment left FreeNets and other kinds of community networks struggling to stay afloat. In general, those that did survive transitioned to function as low-cost ISPs, rather than the community-development organizations that were originally imagined. With the shift to high-speed internet and as

[113] Michael Hrybyk, former director of BCNET, has on a number of occasions recounted a story about being visited by a BC Tel executive during 1995, who told him the company would never offer internet service (G. Graham, personal communication, September 26, 2015; M. Hrybyk, personal communication, May 4, 2016). By 1996, BC Tel had entered the ISP market alongside other telcos offering service under the Sympatico brand (Canadian Press, 1996), and quickly became the province's largest ISP (M. Wilson, 1997).

government-funding proved unreliable or dried up entirely, these organizations had to become sustainable on the basis of regular member contributions (what one Executive Director of the NCF jokingly referred to as “mandatory donation”, Hunt, 2014, p. 61).[114]

Still, FreeNet descendants like NCF[115] continue to play a unique role in society unmatched by commercial ISPs. These survivors have found a “niche” (M. Hrybyk, personal communication, May 4, 2016), serving certain marginal populations as an 'ISP-of-last-resort',[116] and supported by those who prefer a community-based non-profit to an incumbent ISP. NCF depends on volunteers for many basic tasks, and would cease to exist without them. Members who have problems can come into the organization's store-front, and receive a level of personal attention (or “hand-holding”) greater than the customer service provided by commercial ISPs.[117] Those members who pay for connectivity or donate to the organization, support services for those members who cannot. And while the few FreeNets that have weathered the transition to basic low-cost ISPs have limited their efforts in public outreach and digital literacy training, their broad mandate and non-profit status leaves the possibility open to future efforts. Even the original vision of FreeNets as information distribution platforms is far from obsolete. True, there are now a wealth of online sources of information as compared to 1994, but these often lack local context, and there remains ample opportunity for intermediaries to better address the information needs of local populations. For instance, in September 2014 Vancouver Community Network (VCN, formerly the Vancouver FreeNet) launched the Street Messaging Service,[118] which

[114] The pressures faced by FreeNets should also be understood against the backdrop of a broader trend, in which non-profits have been expected to be more “businesslike” in their operations (Bodnar, 2007).

[115] Which remains by far the best-documented of the FreeNets in Canada.

[116] For example, NCF's recent partnership with Ottawa Community Housing (Schnurr, 2016).

[117] This help can extend to kinds of technical assistance that are not strictly an ISP's responsibility (N. Ouzas, personal communication, October 8, 2014; R. Kouhi, personal communication, October 17, 2014).

[118] The project was funded by CIRA (see below), an organization that has recently been supporting a growing

distributes locally-relevant text message updates to street-involved people, particularly in downtown Vancouver (CIRA, 2014).

The public good of private infrastructure

The early FreeNets were based on dial-up access. They took advantage of the existing telephone infrastructure and could be established using modest hardware investments. As the incumbent telecom infrastructure transitioned to high-speed broadband, much of the original FreeNet vision was left in the dust. And yet, this is not because connectivity became more equal across Canadian society. Instead, a new sort of inequality was created based on the distribution of material infrastructure. Certain forms of connectivity were either present or absent in an area, and those who remained on dial-up often had no other choice. Mobile connectivity required towers and spectrum, and all connectivity was now underpinned by fibre-optic backbones. In some areas, fibre-optics were extended all the way to a subscriber's premises, but only where ISPs decided this investment in infrastructure would be worthwhile. Discussions of the digital divide would not vanish as the majority of Canadians gained internet access, but the discussion would remain focused on the material preconditions of connectivity. Even as academic discourse came to conceptualize the problem as being deeper than a lack of physical access (Gurstein, 2003; van Dijk, 2006, p. 230), public policies that had funded various community networking initiatives and social supports for technology use were abandoned (Longford et al., 2012, pp. 10–12). The public policy approach that survived was more narrowly directed toward extending private infrastructure. Access was identified as the ability to choose and consume a private internet service, and the role of public policy would be to create an environment favorable to

number of internet-related projects that in a previous era might have received government funding.

private infrastructure development.

The types of intermediaries considered in the rest of this chapter have a narrower mandate than the early FreeNets or Cybera, and the public policies that have supported them focus largely on physical connectivity. And yet, a broader argument of this dissertation is that the roles of internet intermediaries are not inherently circumscribed, but open to expansion. The fact that the present belongs to the incumbent ISPs and their visions of what an intermediary should be, rather than the socially progressive vision advocated by the FreeNets, is the result of the political economy of internet described in the previous chapter. The dream of the FreeNet remains associated with the era of landline telephones and dial-up modems, but there is no technological reason why the sorts of intermediaries which were imagined in the mid-1990s cannot operate over leased access to fibre-optic cable, or as wireless "mesh" networks (see Antoniadis & Apostol, 2014; Shaffer, 2011).[119] A lot of what we have come to expect from our intermediaries can be thought of as a narrowing of the imagination since the heady mid-1990s, as incumbent commercial networks became accepted as the natural order of things, and public policy was limited to fixing the gaps these networks left behind. Even so, progressive ideas about the social roles that intermediaries could play never vanished, and as described below, have emerged in some exciting new forms.

Publicly-funded regional and provincial networks: Connectivity beyond the urban core

Connectivity, whether defined broadly as encompassing "effective use" (Gurstein, 2003), or narrowly defined as access to material infrastructure, exists in a tension between two

[119] A change in the technological basis of connectivity, such as the shift from dial-up to broadband, does mean that a different regulatory regime comes into play. This regime determines the extent to which infrastructure is open-access, or closed and proprietary, as discussed in the following chapter.

assumptions. The first assumption is that connectivity has at least some of the characteristics of public good, in the sense that it has broad and indispensable public benefits. The second assumption is that connectivity is best provided through private networks as a commodity.[120] However, while privately-funded broadband networks have extended their reach and improved in quality over time, there is no strong incentive for commercial ISPs to extend and deepen connectivity. Such efforts might win these companies more customers, or provide a competitive advantage against inferior networks, but building and updating network infrastructure is costly. The ideal customer base for a commercial ISP is one that generates revenue and does not demand a great deal of bandwidth. As with the issue of universal telephone service in the twentieth century, there are limited reasons for private ISPs to serve remote rural regions, where the costs of building infrastructure either cannot be recovered, or where returns are smaller as compared to urban areas. This has left many rural communities wondering how to improve their situation without waiting for the arrival of market forces (Marlow & McNish, 2010).

Where markets fail to produce the desired outcome, governments are often called upon to step in. But the federal government, which has ultimate authority over telecom in Canada,[121] has been reluctant to take any bold moves towards improving connectivity in recent years. Unlike Australia's National Broadband Network (the NBN, which has been used as a point of comparison in numerous discussions of broadband policy in Canada), Canada's federal government has lacked the ambition to fund nationwide broadband infrastructure (Rajabiun &

[120] The idea that something can both be a public good and provided by private industry is not unique to connectivity, and has been recognized by contemporary updates of public good theory (Kaul & Mendoza, 2003).

[121] There have been jurisdictional disputes between provinces and the federal government in a number of regulatory hearings, but these have generally affirmed federal authority (Babe, 1990, pp. 131–132; Winseck, 1998, pp. 239–241).

Middleton, 2013, p. 9).[122] The absence of leadership by the federal government on this issue has been symbolized by the long delay of a national digital strategy (Geist, 2014a; Wolfe et al., 2014), which, when finally released in 2014 (Government of Canada, 2014), lacked much in the way of strategic vision (Geist, 2014a). Federal and provincial governments have recurrently provided one-time funding for specific broadband infrastructure projects, but these have typically had a limited focus, such as seed money for a local ISP in an underserved town (Industry Canada, 2014c; see Rajabiun & Middleton, 2013). These grants have worked to plug individual holes in broadband connectivity (Van Gorp & Middleton, 2010), but my focus in this section will be on the larger investments in networks that seek to cover the population of entire provinces or substantial portions thereof.

In the absence of federal support, a number of provinces and regions[123] have pursued their own broadband strategies. Some provinces have partnered with local ISPs (with government and industry splitting costs) to extend internet access to underserved areas. In 2006, the Nova Scotia government pledged to bring universal internet service to the province by 2009. Funding for Broadband for Rural Nova Scotia (BRNS) was split between the provincial and

[122] There were bold visions put forward for a national broadband plan from the mid-1990s to the early 2000s, the most notable of which was the National Broadband Task Force's recommendation in 2001 for a multi-billion-dollar investment in infrastructure to extend broadband to all communities (National Broadband Task Force, 2001). The recommendation was not implemented, and federal government programs since the mid 2000s have been modest in comparison to earlier plans and other countries' national strategies (Van Gorp & Middleton, 2010, p. 218).

[123] Active regional networks include the Columbia Basin Broadband Corporation (http://www.cbt.org/initiatives/broadband/), Eastern Ontario Regional Network (www.eorn.ca), the Niagara Regional Broadband Network (www.nrbn.ca), the London and Region Global Network (www.largnet.ca/), the Windsor-Essex Development Network (http://www.wednet.on.ca), Internet Papineau (http://www.ipapineau.net), Réseau Picanoc.net (http://www.picanoc.net), with plans for a regional network underway in south-west Ontario (http://swiftnetwork.ca/). There have also been a number of publicly-funded regional projects to improve connectivity for First Nations communities (Fiser & Clement, 2012; R. McMahon, 2013; R. McMahon, Gurstein, Beaton, O'Donnell, & Whiteduck, 2014; Ministry of Northern Development and Mines, 2010) and the Qiniq network (https://www.qiniq.com/) is a satellite network serving all communities in the territory of Nunavut.

federal governments and three private ISPs, and has stalled just short of its goal of achieving 100% coverage (MacDonald, 2014).

Universal service (or 100% broadband penetration) is also a provincial objective in BC,[124] where the government has signed two successive agreements with TELUS to extend broadband service through the province.[125] The most recent of these (the Connecting British Columbia Agreement, or CBCA, signed in 2011) gave TELUS a ten year contract to provide broadband service to various government buildings, but also obliged them to provide mobile connectivity along many of the province's highways, and to build facilities at 119 rural locations where local ISPs could connect to the TELUS network and purchase wholesale connectivity at a predetermined rate (Connecting British Columbia Agreement, 2011). The level of wholesale connectivity ensured by the CBCA is so basic that it is difficult to consider it "broadband" under (Fiser & Clement, 2012; R. McMahon, 2013; R. McMahon, Gurstein, Beaton, O'Donnell, & Whiteduck, 2014; Ministry of Northern Development and Mines, 2010) current definitions of the term,[126] but BC is not the only province in which a public policy to improve rural connectivity has failed to measure up to escalating public needs.

[124] See Connecting British Columbia Agreement 2011, 21. The CBCA's target was coverage for 97% of the population, with the intention of reaching the remaining 3% through satellite services.

[125] The first of these was the Connecting Communities Agreement, signed in 2005.

[126] By the time of the British Columbia Broadband Association Conference in April 2014, the 10 Mbps wholesale connectivity mandated in the CBCA had become quite inadequate (this would allow approximately two devices in a town to watch high-definition Netflix simultaneously), and many of TELUS's connections had been upgraded to 30 or 100 Mbps. Participants in the room expressed the concern that even 100 Mbps was proving inadequate. Bandwidth usage has climbed steeply in recent years due to streaming video consumption, and the CBCA's is just one of numerous connectivity targets that has become insufficient not long after the network was built to achieve it.

The case of the SuperNet: Profiting from policy

> "*We make money when the government gets its policy outcomes*."
> -Art Price, CEO of Axia (Collison, 2003, p. 3)

Alberta's SuperNet has been one of the most ambitious attempts to steer connectivity towards public ends in Canada. Its design represented a bold new model of broadband infrastructure provision, but SuperNet's history is symptomatic of the tensions that result when commercial ISPs are used as instruments of public connectivity. The project arose at the end of the 1990s from a need to connect government and public buildings (such as schools and medical facilities) across the province, combined with the idea that the same network could be used to extend rural connectivity, enabling economic development beyond the cities, and bridging the digital divide (Collison, 2003; G. Fletcher, personal communication, July 20, 2013; Kozak, 2010; Unland, 2000).[127] As in BC's subsequent agreement with TELUS (see above), rural development would be achieved by establishing local interconnection points in specified communities, where ISPs could connect to the network and buy wholesale internet access. These ISPs would then sell internet access across the 'last mile' to individual subscribers (homes and businesses) at standardized rates comparable to urban centers, thereby eliminating the "distance disparity in cost between rural and urban Alberta" (Government of Alberta, Bell Canada, & Axia SuperNet Ltd., 2005, p. 562). As in BC, the government would not end up owning a network, but paying to

[127] Also among the government's hopes was the development of a new ICT-based knowledge economy for the province, which might even attract Silicon Valley businesses to move north (Wire Report, 2000a). Kozak (2010) has identified four possible explanations for why the Alberta government decided to have the SuperNet built: First, the project a "historical pattern of government intervention in infrastructure development in Alberta and a desire to be seen as visionary and technically advanced" (p. 59). Second, "to provide new economic development opportunities for rural Albertans" (p. 61). Third, a "desire to be, and to be viewed by other governments as, technologically advanced" (p. 62). And fourth, a massive government surplus from oil revenues meant that "the province, unlike all of the others, could afford to build a fiber-optic network that spanned the province" (p. 67).

align a privately-owned network with public policy objectives.

The SuperNet was based on the rationale that a competitive market could meet public demands and government needs, and government's role in the prevailing liberal ethos should be limited to ensuring that a competitive environment existed. But it was clear that the telecom industry in Alberta had no interest in building the sort of network the government imagined, unless there was some additional profit in meeting these public policy objectives. A government owned-and-operated network was out of the question, given the policy orientation through the 1990s of privatizing provincial infrastructure wherever possible and promoting competitive markets (D. Mitchell, 2007, p. 267).[128] Instead, the government offered to fund much of the initial cost,[129] and in February 2000, Alberta's Ministry of Innovation and Science sought bids from private partners who could contribute the remainder of the capital as well as operate the network. The winning bid was submitted by a consortium in which Bell was the major contributor, as the company was seeking to make inroads into a region that had long been served by TELUS's previous incarnation as a government monopoly (Collison, 2003, p. 4; Marck, 2007).[130] However, the operator of the SuperNet would not be Bell, but Axia, a small Calgary-

[128] Kozak (2010, p. 53) has described the Alberta government as "generally under the sway of neoliberal ideology" and adhering to "its ideological proclivities by contracting with private partners" for the SuperNet project. This led to "ministers seeing the network as a contract to be adhered to rather than a policy", and meant that documentation pertaining to the project, including the agreement between Axia, Bell and the provincial government, has been treated as confidential information (see Marck, 2005). Government Ministers actively worked to keep information about SuperNet private, with "government paranoia" about publicity leading to documents being filed as reports to the Minister so that they would not be subject to FOIP (Kozak, 2010, p. 84).

[129] In the end, the government contributed $193 million to the network build, and committed to a ten-year contract to purchase telecom services (Government of Alberta, Bell Canada, & Axia SuperNet Ltd., 2005, p. 562).

[130] TELUS was formed as a result of the privatization of Alberta Government Telephones (AGT) and a merger with BC Telecom. It was considered a favorite to win the SuperNet contract given its close history with the provincial government. The decision to award the contract to the Bell-Axia consortium was justified on the basis of its superior and "innovative" bid (Rubinstein, 2001), but some have speculated that TELUS angered the government by relocating its headquarters to Vancouver in 1999 (F. Fraser, 2008). While local partner Axia lacked the scale and expertise of the incumbents, it was hardly an outsider to provincial politics, being headed by the "well-known" former CEO of Husky Oil (Scotton, 2001; see also Alberta Venture, 2007).

based company with no experience building or operating such infrastructure (D. Mitchell, 2007, p. 267).

The results of the SuperNet project have been mixed for the province of Alberta. Some promotional materials claim to “have made global connectivity available to all Albertans”, removing “most of the technological barriers” and leaving imagination as the only limit to this “broadband superhighway” (Government of Alberta et al., n.d., p. 3). It is clear that public facilities across the province[131] have benefited from connections to SuperNet. Many rural schools would likely still be waiting for market forces to bring them affordable connectivity had the government not initiated the project. But in recent years public sector clients have been growing frustrated with the network, with some switching to cheaper connectivity from an alternative upstream source (Dobson, 2016, p. 16; Krajewski, 2017). SuperNet has also not had a transformative impact on rural Alberta, and as of 2012, well over a hundred rural communities with a SuperNet connection had no ISP using the network to provide last-mile services.

Critics allege that the network is underutilized, and should be opened to broader access (Alberta Economic Development Authority, 2010; Cybera, 2014a, pp. 3–4; Gignac, 2011). The most commonly-identified shortcoming of the SuperNet model relate to the costs required for private ISPs to use it serve rural areas. These include complaints about the rates charged for broadband over SuperNet (Calgary Regional Partnership, 2015, p. 6; Cybera, 2014a), but primarily, it is the cost of setting up an ISP to cover the 'last mile' between SuperNet and individual homes and businesses that has proved to be the main obstacle preventing greater use of the network to serve non-government subscribers (Agriculture and Rural Development, 2009, p. 31; Bull, 2017, p. 20; Gignac, 2010; Wolfe et al., 2014, p. 5). Extending last-mile service

[131] Some 3,300 schools, hospitals, libraries, provincial government and municipal facilities (Bull, 2017, p. 4).

through SuperNet is simply not profitable enough to justify interest from private industry in large parts of rural Alberta, and for those residents and local governments that have wanted to take connectivity into their own hands, lack of expertise and available capital have presented major challenges (see below).

Since 2009, around $25 million has been contributed by the provincial government in two waves of funding to a variety of local connectivity projects, some of which have helped plug the gaps in SuperNet's last mile (Alberta Agriculture and Rural Development, 2014; Government of Alberta, 2012; Rajabiun & Middleton, 2013, p. 14).[132] But the provincial government's attention to SuperNet has been inconsistent, divided between departments, and frequently absent.[133] The provincial government largely let its private-sector partners (principally Bell and Axia) sort out the details of the network, and dysfunctional relationships between these companies contributed to the "tortured history" of SuperNet's first years (F. Fraser, 2008). These include a set of disputes between Bell and Axia during the building phase of the network that delayed its completion and led to changes in the responsibilities of the project's private partners (*Axia Supernet Ltd. v. Bell West Inc., ABQB 195*, 2003; Collison, 2003, p. 4; Gignac, 2003). Further disputes followed in 2010 and 2013, with Bell and Axia initiating arbitration proceedings against the other over failures to meet obligations under the SuperNet Agreements (Axia, 2011, p. 24,

[132] TELUS has also used some of $99.4 million in its CRTC-mandated "deferral account" (see Nowak, 2010) to improve connectivity in Alberta communities that had a SuperNet connection, but no active ISPs serving the community (AAMDC, 2011, p. 43). TELUS was successful in arguing (against Axia's objections) that it was not required to use the SuperNet to provide connectivity in these communities (CRTC, 2011a; The Wire Report, 2011).

[133] In a 2011 article about the SuperNet and rural broadband, Alberta Premier Alison Redford was quoted as saying: "we haven't focused on it as a priority ... (It) seems to have been more of a problem between government departments not wanting to take ownership, or not knowing exactly who's the leader" (Gignac, 2011; see also Wolfe et al., 2014, p. 5).

2013, p. 11).[134]

The SuperNet's design, which includes the contractual obligations of its parties, was one of “open-access” infrastructure which any ISP could take advantage of (Wire Report, 2000a). But TELUS, which maintains Alberta's most extensive last mile infrastructure, did not utilize SuperNet in this manner, preferring to use its own facilities even where this meant incurring the expense of constructing duplicate infrastructure alongside SuperNet (CRTC, 2010b).[135] The company has also resisted attempts by other parties to link TELUS-owned telephone infrastructure to SuperNet (CRTC, 2009a; F. Fraser, 2008; Rajabiun & Middleton, 2013, pp. 14–15), so that local ISPs wishing to take advantage of SuperNet have had to build their own last mile infrastructure, rather than using TELUS's copper network. Axia's role as the SuperNet's “operator of operators” (Government of Alberta, 2005), was to ensure the network's openness to whatever ISPs wanted to make use of it. But in recent years the company has increasingly moved to address SuperNet's last-mile failings by providing this missing piece of connectivity itself.[136] Far from being content to serve as the SuperNet's neutral and contractually-delimited middleman, Axia (specifically, as Axia Connect Ltd.) has become a leading builder of fibre-to-the-premises networks in rural Alberta by working with connectivity-hungry communities (Axia, 2015, 2017).

[134] Bell argued in late 2010 that Axia should not be using SuperNet to provide a new wholesale service (Axia, 2011, p. 24), while Axia claimed in 2013 that Bell should be using SuperNet for commercial traffic in rural Alberta (Axia, 2015, p. 17).

[135] According to Axia's CEO Art Price, TELUS does make some limited use of SuperNet in Northern Alberta where it does not make economic sense to extend their network, but in these remote regions TELUS will “first go to Ottawa and see whether they can get more money to add to their own backbone... and only after the answer is no do they come to us” (CRTC, 2016b, paras. 10961–10970).

[136] Axia SuperNet Ltd.'s contract with the Alberta government to sell wholesale bandwidth to local ISP through SuperNet prohibits the company from competing with these service providers by serving customers directly. However, large “enterprise customers” (such as oil and gas companies) are able to “become Service Providers for their own sites” and thereby qualify as Axia SuperNet Ltd. customers (P. Roberts, 2011). A different Axia subsidiary, Axia Connect Ltd. (both Axia SuperNet Ltd. And Axia Connect Ltd. Are subsidiaries of Axia NetMedia Corporation) provides last-mile connectivity and has been developing fibre-to-the-premises projects in a number of rural Alberta communities (see CRTC, 2016b).

In summary, the Alberta government has tried to extend rural connectivity through open access to a fibre-optic network which connects to public buildings around the province. The main obstacle to rural connectivity has been the lack of a “business case” for ISPs to cover the costs of required infrastructure. The government's solution was a one-time contribution to fund a fibre-optic backbone for the province, and to specify the terms under which this backbone would operate. Where the market failed, government stepped in, but only to the extent necessary to create the conditions which would allow a competitive private industry to flourish. A for-profit 'middle-mile' ISP (Axia) would manage and operate the network, selling wholesale bandwidth to all other ISPs, and effectively becoming a private-sector steward of public connectivity. The company would be contractually aligned with public policy objectives, such as equivalent pricing for rural and urban areas, and open access to last-mile ISPs. In this case, market failure was not used to justify public ownership and management, but an attempt to reconstitute the market. Private companies, enabled by the right contractual obligations and pricing structures, would meet the need for rural connectivity through their own initiative. Axia would profit by meeting the government's public policy objectives, and other ISPs would spring forth to plug gaps in rural connectivity once the economic opportunity manifested.

The idea of a middle-mile ISP acting as a neutral gatekeeper and manager of a network open to all comers is a compelling one.[137] In such an arrangement, the role of the state is limited to setting and enforcing the terms under which the network operates, keeping the network's operations in private hands. The question then becomes how to best ensure the autonomy of

[137] This kind of arrangement is also known as “structural separation” is discussed in the following chapter (a related concept, “functional separation” also separates the company providing wholesale from the retail provider, but allows for common ownership of the two). Such networks, in which one party is limited to managing a middle-mile wholesale network for the common benefit of other actors, have been implemented in several countries, most notably the UK (see Middleton, 2011, pp. 64–65).

private, for-profit intermediaries, while also channeling their actions towards the accomplishment of public policy objectives. This is especially tricky when public policy seeks to correct a market failure as severe as the absence of broadband service in a given area, since the business incentives structured by the state must be sufficient to create a market where none existed.

The SuperNet story can be read as an attempt to steer private industry towards achieving public policy objectives, by increasing opportunities for profit in rural Alberta.
The rationale was that private ISPs, by doing what businesses do best, would also end up serving the best interests of the province. In time,[138] Axia did indeed become a profitable company, marketing the open-access model developed for the SuperNet around the world and implementing it in France, Singapore, and Massachusetts. But SuperNet did not create the conditions for private industry to extend rural connectivity in much of the province, since a point-of-presence was simply not enough of a foundation for a profitable and competitive rural industry to take off. As a consequence, some rural Alberta municipalities (Marlow & McNish, 2010), regions (Stoesser, 2015), and counties (Kozak, 2010, 2013) undertook their own projects to bring connectivity where the combination of SuperNet and private industry had failed to deliver. The following section will examine efforts by municipal governments to address these connectivity challenges.

Municipal networks

Regional projects like Alberta's SuperNet, the TELUS network in BC, and EORN in

[138] Axia, like Bell (see Marck, 2007), suffered significant financial losses in the early years of the SuperNet project (Scotton, 2001), since the government's contribution was capped and additional expenses had to be covered by the companies.

Ontario[139] are middle-mile networks that provide wholesale connectivity to last-mile ISPs in order to further the public policy goal of improving connectivity. But just as last-mile networks depend on these middle-mile networks to connect to the rest of the internet, a middle-mile network like SuperNet is only a partial solution to the digital divide without last-mile networks being in place to close the circuit with individual subscribers, and it is at this final stage that the costs of network-building are typically greatest.

The material challenges of connectivity become clear when looking at the experience of municipalities that desire better internet access. Often, this means that a last-mile network within the town or city must be built or upgraded. The process can involve digging trenches, installing fibre-optics, and building towers for wireless. These expenditures quickly escalate into millions of dollars, and finding the necessary capital is one of the largest challenges for municipalities looking to improve last-mile connectivity. Additionally, a high-speed municipal network is all but useless if it cannot connect to a larger network that extends beyond the municipality, and which can provide the required connectivity to the rest of the world. These challenges are evident in the remarkable story of Olds, Alberta – a town that was able to extend a fibre-optic network throughout the municipality at great cost, maximizing connectivity through a 'gigabit network' that promises to exceed the connectivity available to most urban Canadians. But it should be noted that municipal networks have typically been pursued through other, less ambitious models, which I will discuss after considering what we can learn from Olds' experience.

Wiring the Town of Olds

Olds is an Alberta town, south of Red Deer, of some 9,000 residents. It sits adjacent the

[139] See note 123 above.

province's main north-south highway and the numerous fibre lines that connect Calgary and Edmonton. The town hosts a college, expanding residential developments, numerous businesses, and volunteer organizations. While Olds has struggled with the challenges of rural economic development and relative geographic isolation, it is greatly advantaged in comparison to most rural Alberta towns. The story of the Olds fibre project is therefore not one of a community stuck on the wrong side of the digital divide, struggling to remain competitive and attractive, but of a town with the resources and leadership required to innovate and invest in a major piece of public infrastructure. Fibre was built in Olds not because the town was starved for connectivity, but because the town had the social infrastructure in place to plan and deliver on a long-term network infrastructure project.

Initial discussions began in 2003, with the Olds Institute for Community and Regional Development (OICRD)[140] forming a Technology Committee to pursue opportunities related to the future arrival of the SuperNet in town, and to "facilitate the community development of a true high quality high bandwidth network to encourage the development and utilization of a fiber optic network to allow access to ICT applications as enablers to the economic and social development of [the Olds] region" (OICRD, 2011, p. 96). The project would have two principal

[140] The OICRD (usually referred to as the Olds Institute) is a volunteer-driven non-profit economic and community development organization founded in 2001. The original board members are the Olds and District Chamber of Commerce, Olds College, Olds Regional Exhibition and the Town of Olds (OICRD, 2011, p. 6). As one former chairman described, it was meant to get the city away from the three-year cycle of small town governance and the "fickle" political leadership that can result (Digital Futures Symposium transcript, November 14, 2013). The OICRD is not part of the city administration, but maintains close ties to the municipal government. It has therefore been able the shepherd the fibre project over the long term, while taking advantage of some of the funding opportunities (provincial loans) available to municipalities. O-NET's revenues are used to repay the loans that the Town of Olds obtained to fund its creations, and can also be used by OICRD (O-NET's only shareholder) to fund other community and economic development projects (Settles, 2012, p. 71). Therefore, it is far from accurate to call O-NET a municipal government initiative (the term favored by O-NET and OICRD is "community owned"), but the network was established to serve the collective interest of the Town of Olds.

champions[141] over the years to come, and while both individuals had local business expertise, neither knew much about telecom other than the fact that the internet would be an important economic and social enabler in the years to come. As one of the project champions put it, “we thought, well here’s the SuperNet, we’ll go out and buy this big extension cord and just plug it in right. And they would bring us the world” (Digital Futures Symposium transcript, November 14, 2013). Not only was there a lack of telecom expertise within the town of Olds for such a project, but no successful 'community network' in Canada had ever been as ambitious. The Technology Committee sought advice from Eastern Canada, where non-incumbent broadband initiatives had a greater history, and from the US, where a growing number of municipalities were investing in broadband. In addition to external consultants, the Technology Committee also sought the participation of the experienced telecom incumbents that were already present in the town (Shaw and TELUS), as well as Axia (operators of the SuperNet). Early on, the plan was for Olds to build an 'open-access network', or 'dark fibre' that could be leased by service providers to offer broadband, telephone, or television to subscribers. In the end, no incumbent partner was willing to provide services over a network built by the town, and Olds was left largely on its own (Settles, 2012).[142]

Rather than the narrowly-focused infrastructure-based intermediary which could be used to extend incumbents’ services, the Technology Committee decided that Olds’ fibre network would need to out-compete the incumbents to be successful.[143] In other words, Olds’ municipal network would need to be a full-service ISP that more closely resembled the model of the

[141] Joe Gustafson and Stirling McLeod, see note 148 below.

[142] Negotiations progressed furthest with TELUS, but were ultimately unsuccessful between 2006 and 2007. Axia contributed to different aspects of the project as a contractor and by volunteering expertise (OICRD, 2011, p. 8).

[143] This meant getting into the business of providing its own 'triple play' (broadband, telephone, and television) services over the network (OICRD, 2011, pp. 98, 112; Settles, 2012).

incumbents, but built using the latest fibre-optic technology. It would have to develop a competitive rationality that would succeed in the local telecom market, benefiting from the advantage of being locally based, but lacking the expertise and infrastructure of established ISPs. This opened a new host of challenges and opportunities for mis-steps, such as developing viable business models for residential subscribers, managing customer service, and arranging the appropriate content offerings and interfaces (see Everest, 2014b; OICRD, 2013). While the role envisioned for the ISP expanded along some lines, it had to be narrowed in other ways, such as the early decision to narrow the scope of the fibre build from the surrounding country to the town itself.

Through a process of trial and error, wrong turns and dead ends, Olds Fibre Ltd. and its O-Net brand gradually took shape.[144] For much of its development, the plan for Olds' last-mile network was to connect to the middle-mile SuperNet, but as time went on it became clear that SuperNet would be too expensive for anything other than an emergency backup.[145] The province’s network was a poor fit for the town’s network. Instead, O-Net leased a fibre connection to Calgary, where it was possible to take advantage of cheaper bandwidth rates.[146] The network was completed in 2015, with the remaining challenge of attracting enough subscribers to cover its cost and begin contributing revenue to the community (OICRD, 2015, pp.

[144] O-Net was formally launched in July 2012 and made available to all residents of the town in subsequent years, but there have been delays in building the network and reaching households that want to be connected. Challenges have included problems finding skilled labour (Chung, 2013), materials, poor performance by certain contractors or partners, and weather (OICRD, 2013).

[145] As one of the project champions explained, “we at Olds simply would not be able to do what we are doing, if I was forced to hook onto the Alberta SuperNet. And that to me is a sad, sad story, but it's a reality” (Digital Futures Symposium transcript, November 15, 2013).

[146] Specifically, O-Net took advantage of the arrival of Hurricane Electric in Calgary's DataHive in 2013 (C. Dobson, personal communication, March 6, 2014; OICRD, 2015, p. 6), which provided an alternate source of low-cost bandwidth for anyone able to connect to the facility. Hurricane Electric's point-of-presence (PoP) in Calgary has been called a “game changer”, due to the way that it dramatically changed the economics of broadband in Southern Alberta, reducing upstream bandwidth costs from around $10 per Mbps to roughly $0.60 for anyone who could connect to DataHive (Digital Futures Symposium transcript, November 14, 2013).

3–5).

Even at the start of 2018, it remains too early to say how much of a success O-Net will be financially or in terms of other benefits to the community, although it has already made a significant impact through national news and social media, and its champions have fielded queries about their experiences from other communities across the country that are also interested in the pursuit of greater connectivity (Everest, 2013, 2014a; Gignac, 2013; OICRD, 2015, p. 7; Sepulvado, 2014). O-Net became a paradigmatic example of what an empowered community can do in the pursuit of greater connectivity, but it also demonstrates what is required to realize such a goal. As an infrastructure project, the Olds fibre network has required pulling together some $21 million dollars over the years from various sources (Gall, 2015; Ho, 2014),[147] in addition to the challenges of actually building and operating the network. What allowed the project to proceed this far (including numerous mistakes and various costly missteps), was steady, determined leadership, and a supportive relationship with other actors – most importantly the governing node at Olds' Town Hall, which acted as a sovereign sponsor.

Given its long and troubled birth, O-Net is far from an ideal case of a community-owned and operated ISP, and most recently OICRD is attempting to refinance its loans related to the project after encountering cash flow problems (Bartleman, 2017). Whether or not the network proves financially successful, the process by which O-Net ultimately became an operational entity shows how "municipal broadband is a very social affair and this aspect will make or break the project" (C. Dobson, personal communication, March 6, 2014)."[148] The case of O-Net

[147] This includes a $2.5 million Alberta government grant, a $6 million loan (Chung, 2013), a $4 million line of credit backed by the town of Olds (OICRD, 2013), and most recently a loan of $8 million (OICRD, 2015).

[148] Furthermore, according to someone intimately involved in the project since 2009, this social aspect "breaks into at least two components. First, you need sound, consistent, committed leadership – the [Olds fibre] project was

demonstrates the challenges of establishing a community-based node to advance local connectivity, as well as the impossibility of pursuing such a project truly independently. This fact is echoed by other small Alberta municipalities grappling with the problem of improving broadband connectivity and encountering internal leadership challenges, with town councils that lack long-term commitment and an understanding of broadband issues, as well as a broad lack of telecom expertise in rural areas (Wolfe et al., 2014).

Models for municipal broadband across Canada

Olds is hardly unique in Canada as a municipality that has pursued improved connectivity as a public policy objective. It is unique in how it has pursued this objective – by establishing an institute for economic development (the OICRD), which conceived of and founded a municipal ISP that extended a fibre-optic network throughout the town, and then offered its expertise and online services to other Alberta municipalities (Calgary Regional Partnership, 2015; Collie, 2015). However, many other models of municipal intermediaries exist across Canada, including the business/government co-operative of Fredericton (Richard & Philpot, 2013; Settles, 2012), and a number of municipally-owned ISPs of varying scope and scale.[149] In Alberta, multiple

largely driven by Joe [Gustafson] and Stirling [McLeod] together with their Technology Committee and they've been at it 10 years. Second, you need strong, supportive community involvement and that enabled via the OICRD structure is excellent in that it fosters very close relationships between the town, its businesses, and residents... Less dominant factors include access to sufficient patient capital (these projects are capital intensive and cash-flow doesn't begin until after the money is spent), sound guidance (on both the technology and business fronts), and some luck." (C. Dobson, personal communication, March 6, 2014).

[149] Six other co-operatives act as ISPs in a region west of Kitchener and north of London, ON (http://www.cni.on.ca/). Other examples of co-operatives include CSUR (http://www.csur.ca/) and CoopTel (http://www.cooptel.qc.ca) in Quebec, Access (http://www.myaccess.ca/) in Saskatchewan, and a group of natural gas co-ops that formed Corridor Communications (http://cciwireless.ca) in Alberta. Municipally-owned ISPs of various kinds also exist in Cochrane, ON (http://www.puc.net/), Granisle (http://granisle.ca/business/granisle-in), Kingston (http://www.utilitieskingston.com/Networks), Kincardine (http://www.brucetelecom.com), Muskoka (http://www.lakelandnetworks.com), Stratford (http://www.rhyzome.ca/), Sudbury (http://www.agilisnet.com/en/), Thunder Bay (http://www.tbaytel.net), and

communities have recently signed or pursued agreements with Axia to extend fibre-optic networks in their communities (Axia, 2017; Whalen, 2013). Such efforts lack the ambition or comprehensive municipal coverage of O-Net, but also do not require the same amount of long-term leadership commitment and capital expenditure. Instead, municipalities rely on an experienced private partner to build, own, and maintain the network.

The different forms of government support for municipal broadband can be distinguished into three broad types, which can be arranged along a scale of lesser to greater municipal involvement (Bower, 2012; see also Dyrda, 2016, p. 8), or different governing rationalities concerning the relationship between public and private actors. In the first, a municipality enters into an agreement with a private ISP, granting access to municipal infrastructure (through a "municipal access agreement") or otherwise providing the ISP with certain rights, guarantees, or contracts, in exchange for the ISP meeting certain municipal goals. In the second model, the municipality deploys its own telecom infrastructure, and leases its excess capacity to private ISPs (for instance, as 'dark fibre', see below). In the third model (as pursued in Olds), the municipality builds a network and establishes an ISP, serving residences or businesses directly. However, many such networks only serve particular classes of customers, such as businesses or other institutions. Urban municipalities in particular do not generally extend connectivity to residential subscribers, leaving these customers for the private sector.

All three of the models listed above can begin from a government's initial desire to connect municipal facilities, followed by the realization that the same infrastructure used to link

Tillsonburg (http://www.rapidfibre.ca). There have also been numerous Canadian examples of municipally-owned ISPs or fibre networks that have failed, or had their assets sold to private industry (Atria Networks, 2008; Calabrese, 2013; Curri, n.d.; Dobby, 2013; Goetz, 2014; The Guardian, 2015; C. Litschko, personal communication, March 28, 2014).

public buildings could be used to improve connectivity within the municipality. After all, a city or town includes various municipal facilities, and there is considerable benefit in having these buildings networked. Local incumbents can usually meet a city's telecom and networking needs, but more than one set of municipal administrators has decided they could reduce costs by building and operating such a network themselves, or entering into an agreement with a private partner to build and operate such a network (Digital Futures Symposium transcript, November 14, 2013; Wire Report, 2000b). Because the cost of installing a hundred strands of fibre is trivial in comparison to the costs of digging up the streets, a network built for a narrow municipal purpose can easily be installed with greater capacity than necessary and then utilized in other ways (City of Calgary, 2014b, p. 7), like connecting other sorts of sites that happen to lie near its path. This approach doesn't generally result in a last-mile ISP with complete coverage,[150] since a municipality begins with the limited ambition of connecting particular kinds of sites. It is a radically more expensive step to extend such a network to cover all the possible kinds of endpoints (homes and businesses) within a city, where capital costs quickly reach tens or hundreds of millions of dollars.

One example of such an intermediate model can be seen in the Vancouver suburb of Coquitlam and its municipally-owned network, called QNet.[151] Unlike O-Net, QNet it is not an

[150] There are exceptions, particularly in the US, the most famous of which is Chattanooga, Tennessee. There, the municipally-owned power company saw benefit to running a fibre-optic cable to each of its customers to better control the power grid, and also realized that they could sell internet access over this infrastructure (Rushe, 2014; Wyatt, 2014).

[151] QNet began as an effort to connect Coquitlam’s traffic lights together, with the network extended to municipal buildings in order to reduce the cost of relying on incumbent telecom services in 2004. The city installed more fibre strands than it required underneath its roads (since the actual material of fibre-optic cabling is a relatively minor expense in such a project compared to labor and construction costs), and then explored how best to “leverage” this asset. After exploring several models, QNet was established and began leasing dark fibre in 2008. The goals of QNet include saving costs and generating revenue for the City, decreasing the impact on rights-of-way by reducing the need to dig up public streets, economic and business development through access

ISP that serves individual subscribers and was never meant to reach all residents of the city. Instead, the city operates a fibre-optic backbone that private ISPs can pay to use in order to serve their customers. The QNet model is that of an 'open-access' network, meaning that the infrastructure is open for various ISPs to provide services over.[152] In other words, the municipality installed 'dark fibre' under its roads, and various parties can pay to 'light' this fibre, or obtain leased access to the infrastructure. Calgary has undertaken a similar dark-fibre approach (City of Calgary, 2014b), and some version of this model is employed by other municipalities, particularly in Western Canada (City of Kamloops, 2015; City of Kelowna, 2015; City of Nelson, n.d.; City of Penticton, 2014, p. 151; McManus, 2015; Wiest, 2014, p. 9).

So what kind of governing nodes are municipal ISPs? What sets them apart from private-sector intermediaries? What is the rationality of these actors, or what ends do they govern or expand their networks? In some cases, the differences can be minor. Municipal ISPs can be organized along corporate lines, and run to maximize revenues.[153] But they are often much more

to fibre, enabling increased competition for local telecom services, and providing connectivity to local schools. As in Olds, the role of a long-term project champion was key in preparing a plan for such a unique business venture, and in gaining and maintaining the support of local leadership. However, instead of being spearheaded by members of a not-for-profit community organization such as OICRD, the project was championed by the manager of the City's ICT department (Rick Adams). QNet is incorporated as a “local government corporation” in BC. It is owned by the city, operates for-profit, is exempt from income taxes, but is restricted to operating in Coquitlam. While “arm's-length” from government, it can take advantage of services offered by municipal departments, such as financial services and civil engineering. This, and the limited nature of its services (dark fibre), means it can operate with minimal overhead and staff. As in Olds, there was reluctance by some incumbents to use the QNet's network. However, over time, more and more ISPs have signed up to lease its dark fibre, and the network is now cash-flow positive and projected to repay the approximately $5 million loan from the City that established it by 2028 (Rick Adams, 2014; R. Adams, personal communication, November 8, 2013; Rick Adams & Coert, 2014; R. Coert, personal communication, November 4, 2013).

[152] ISPs are not the only customers of dark fibre networks. Mobile networks also need wired connectivity to their towers, and institutions that utilize a lot of data, such as large businesses or schools, also lease fibre to deliver their traffic to a preferred service provider or data center.

[153] One manager of a municipally-owned ISP (Lakeland Networks, which grew out of a power utility) attributed the decision to expand into internet services to an “entrepreneurial point of view”, and described the choice of whether or not to extend services to particular customers (who may be expensive to connect) as ultimately a “business decision” (C. Litschko, personal communication, March 28, 2014). A similar entrepreneurial spirit can be seen behind the development of O-Net (S. McLeod, personal communication, March 14, 2014), and

than profit-generators, and their champions may be government bureaucrats, social visionaries, or dissatisfied citizens convinced that they can do better than what is offered by private industry. Municipal ISPs or 'community networks' (including co-operatives) are often guided by notions of collective interests or the public good. This is essentially the argument made by the City of Calgary before the CRTC in 2014, to argue that as public institutions, municipal ISPs should be treated as a distinct “government class”, and “forborne” from (not subjected to) the same regulations as commercial ISPs (City of Calgary, 2014b).[154] Municipal governments exercise limited sovereignty over local affairs that is circumscribed by higher levels of government (including the CRTC), but they are explicitly mandated to operate in the public interest, and to serve all of their citizens, echoing some of the concerns around equitable connectivity and the digital divide described earlier in this chapter.[155] While few municipalities see their role as ensuring that every citizen has access to broadband, many recognize that telecom is interrelated with a host of collective or public concerns, such as social and economic development,[156] and management of rights-of-way, or other physical infrastructure (roads, power, water).[157]

municipal networks must often be justified on the basis of a “business case” or “return on investment” (Digital Futures Symposium transcript, November 14, 2013; Hovis, 2013). This indicates the economization of connectivity and the adoption of a business rationality in government. However, proponents of municipal networks also often argue for the need to conceive of benefits and “returns” beyond narrow economic terms, and inclusive of broader social benefits (see Dobson & Graham, 2016; Hovis, 2013; Longford et al., 2012; Tapia & Ortiz, 2008b).

[154] Specifically the City of Calgary (2014b) argued that instead of providing services for profit, “municipalities provide municipal services in the best interest of their residents”, including serving residents where this might be unprofitable for the private sector. Hence, municipal networks can “support and complement the networks of commercial carriers” (p. 3), and should not be regulated the same way.

[155] In its 2014 submission to the CRTC's proceedings on wholesale access to fibre-optic networks, the City of Calgary argued that “municipal governments are mandated to provide services to all citizens, regardless of location or economic benefit. Commercial carriers do not have sufficient incentive to bring fibre to every community if it is not profitable, which leaves some communities disadvantaged. Municipal fibre can complement the fibre networks of commercial carriers” (City of Calgary, 2014b, p. 7).

[156] This can mean being selective about what parties the city does business with, aside from practical or business considerations. For instance, the City of Kamloops (2015), states that dark fibre from its network “is available by lease to customers who can demonstrate economic or other benefits to Kamloops.”

[157] (see City of Calgary, 2014b; City of Ottawa, 2003; R. Coert, personal communication, November 4, 2013;

The challenge of public connectivity

Unlike private firms, public intermediaries such as those discussed throughout this chapter can be established with the explicit purpose of serving public policy objectives, but these goals are as open-ended as the public interest itself,[158] and place few limits on the possibilities for these institutions. A municipal intermediary or regional network can be founded to bring broadband into the lives of all citizens, to support innovative social programs and technologies, or to invigorate rural communities. Politics can be a forum for a diverse range of interests, and the values and rationality that guides the public pursuit of connectivity cannot be foreclosed. Private industry selectively deploys networks where profitable, but public agencies work to fill the gaps, guided by the view that connectivity is too important for the disadvantaged to await 'the market'. Where private industry maximizes profits, public connectivity projects might increase public revenues, but are just as likely to encompass notions of collective development, local autonomy, equitable and accessible connectivity, or the cultivation of particular populations (such as young professionals and 'knowledge workers').

Returning to the guiding questions posed by the nodal governance approach in the introduction[159] we can appreciate intermediaries' particularities and the challenges of generalizing across the institutions considered in this chapter, which span a variety of organizational forms. When resources and support are provided from public sources, intermediaries are accountable to the sorts of outcomes and terms specified by these

Federation of Canadian Municipalities, 2009).

[158] At its worst, the public interest is equated with the interests of public institutions, and anything that benefits these institutions is justified as a benefit to the greater whole. Commercial ISPs also sometimes justify their actions as being in some formulation of the public interest. Most frequently, this is when their actions align with public policy, such as when companies invest in new facilities (see Rajabiun & Middleton, 2015, pp. 51–52).

[159] Who are the actors? What are their capabilities, rationalities, forms of knowledge, outcomes/ways of measuring success, and relationships with other institutions? (Wood, 2006, pp. 230–231).

arrangements, such as connecting remote or disadvantaged populations (the CBCA), or serving public sector clients (RENs, SuperNet). A few public intermediaries, such as O-Net, are partly guided by a competitive rationality that pits them against private industry, but public intermediaries typically compete in a carefully delimited way within a narrow market (public sector clients, dark fibre, regional transport).

Public intermediaries' dependent links to state agencies can be as recipients of funding, beneficiaries of special regulatory treatment, or intermediaries may operate under the auspices of a public authority (as QNet operates under the City of Coquitlam). Even when the intermediaries are non-state or civil society organizations seeking to promote local autonomy, this is typically only possible within a framework defined by state institutions and by mobilizing other governing nodes, such as municipal, regional, and provincial government agencies. Finally, because they are often in a marginal position in telecom's political economy and are less likely to see each other as market competitors, public institutions can cultivate cooperative relationships which one another, where they confront common challenges, benefitting from combining efforts or interconnecting networks.[160]

This chapter has demonstrated how adaptable intermediaries can be to various public policy objectives and how the dream of connectivity can promote locally distinct values. I will return to these ideas, and the possibilities engendered by alternative models of connectivity, in the concluding chapter. However, it should be noted that while there are numerous examples across Canada of internet access being treated as a public good, the various dreams and desires attached to connectivity can exceed what is achievable, and project outcomes often fail to meet

[160] In Alberta, such collaborations have been developed through Digital Futures Symposiums held since 2013, and plans have also been advanced through the Calgary Regional Partnership (2015).

expectations. Many planned public networks were never realized, some were sold to private industry after completion, or (like SuperNet) fell well short of the transformative rationale used to promote them. Relative successes, like O-Net, are a testament to challenges overcome through long-term dedication as well as the presence of fortunate circumstances.[161] However, the material and operational challenges of building and operating networks are not the main obstacles to the spread of connectivity as a public good (whether through community networks or some sort of broadband utility). Rather, it is the very notion of connectivity as a public good that contradicts the governmental rationale underpinning telecom liberalization – that connectivity is best provided through private networks as a commodity.[162] It is this contradiction has become the main obstacle to public connectivity projects, or an enduring source of tension within their constitution.

The tension between public connectivity and private infrastructure is evident in the SuperNet's last-mile shortcomings, recurring debates over how to make a 'basic' level of broadband available to all Canadians (CRTC, 2015c), and the careful line that RENs and networks like QNet have to walk to avoid competing with private ISPs. In all of these cases, publicly-funded networks or government-mandated connectivity run contrary to the rationality that the public good is served by government sticking to what it 'does best', and staying out of realms delegated to the private sphere. Governments have taken this to mean a reliance on market forces wherever possible, with public sector intervention only appropriate where the

[161] A particularly important factor is geographic location and proximity to affordable upstream connectivity. Locally-available expertise is also a major asset, as are stable and supportive governments with access to funding.

[162] One participant in 2013's Digital Futures Symposium expressed the sentiment that, whereas in Europe discussions of broadband are about the "public good", in Canada "business is just almost de facto in the public [interest]... it can do no wrong" (Digital Futures Symposium transcript, November 14, 2013).

market has failed, and even then the preference has been to find ways to align private intermediaries with public goals. While there continue to be calls for greater government involvement in providing telecom services or building and operating networks, these arguments now take place at the margins of public discourse. The assumption is that even if broadband is now some sort of essential utility, it is best provided by the private sector. Exactly what competition means in this context, and how a particular understanding of competition has been regulated into being and imposed on Canadian intermediaries will be the topic of the following chapter.

Chapter 3: Chasing Competition

We all thought that when we got there, when competition happened, there'd be no more regulation. Well, here we are. We're all still have pretty good jobs as... in the regulatory department.
-Ken Engelhart, Senior Vice-President, Regulatory & Chief Privacy Officer, Rogers Communications (CPAC, 2012)

This dissertation deals with the roles and responsibilities of ISPs as instruments of public policy. Among these, no topic has sustained a greater volume of heated debate within Canada's telecom industry than the ways in which intermediaries are regulated in order to promote competition. This kind of regulation goes well beyond the traditional scope of policing anti-competitive (or anti-trust) practices, such as investigating collusion by dominant players or the use of market power to set prices (as cartels, see Davies, 2014, pp. 41–42). Instead, the telecom industry has been regulated in order to create the conditions for a new structural arrangement, in an attempt to reorder the incumbent-dominated telecom landscape inherited from the monopoly era. In short, by setting the rules for how private companies must relate to each other, and granting non-incumbents access to key infrastructure or wireless spectrum, governments have tried to foster a competitive industry. Only once such an outcome is achieved would regulators be able to step back (see Information Highway Advisory Council, 1997, p. 12) and allow market forces to govern.

However, rather than retreating from the market, the CRTC has become ever-more entangled in the relationships between ISPs, regulating the role conflict imposed on companies that are required to serve their competitors, in what I characterize as a state of ‘competitive dependence’. In short, incumbents are expected to provide the means for smaller companies to survive, while simultaneously competing against them. What was meant to be a temporary crutch to help the industry move into a deregulated world has become an enduring constraint on the forces unleashed through liberalization. Early hopes that liberalization would result in deregulation and a free, competitive market, have been replaced by regulations that simply try to keep the power of incumbents in check and preserve something resembling the status quo.

This chapter explains the Canadian telecom regime of 'regulation-for-competition' (Levi-Faur, 1999),[163] its goal of creating competition where it is lacking, and the resulting state of competitive dependence. These developments can be understood in the context of regulatory capitalism, combining aspects of neoliberalism with new forms of state regulation. According to David Levi-Faur, “While neoliberal systems of control are manifested in the marketization of social and economic life, regulation supplies the means to promote, sustain, and control marketization” (2006, p. 497). Competition is therefore treated as a condition that can be regulated into existence through the obligations that participants in the market have toward one another, rather than as an alternative to regulation.

However, a sufficiently competitive market can stubbornly refuse to emerge despite a regulator's efforts. As a result, while regulation-for-competition is still justified as a way to create a sufficiently competitive industry, the more immediate results are limits on the exercise of power by certain actors. Without such limits, further concentrations of power and industry consolidation would predictably follow. In other words, rather than forging a bold new liberalized world, regulation-for-competition has had the more immediate effect of preserving something closer to the status quo, and preventing the ultimate triumph of the giant firm. The

[163] Vogel (1996, p. 17) describes this sort of regime as “pro-competitive reregulation”, in which the goal is to create competition “by offering regulatory advantages to competitors or imposing disadvantages on incumbents”.

mandated access regime has therefore engendered a state of competitive dependency as a middle road between two unacceptable policy alternatives: allowing further concentration of powers or forcing a structural separation of powers.

I argue that the enduring contradictions in regulation-for-competition are the unplanned consequences of failed public policy, but that this failure may yet be redefined as success, as promoting something closer to the existing order. First, I will explain how current expectations of ISPs have been shaped by liberalization, through definitions (and redefinitions) of competition, and delineations between those intermediaries that are expected to compete, and those that are prohibited from doing so.

The idea of competition

There is a tension at the heart of any competitive activity. Participants must be formally equal at the outset, but unequal at the conclusion. Competitors must be constrained by norms of equality, playing by the same rules, but in pursuit of inequality (Davies, 2014, p. 41). In Canada's telecom industry, intermediaries regularly call for a "level playing field" when seeking or opposing various forms of government intervention (Bell, Rogers, & TELUS, 2013b; CNOC, 2013, paras. 147–149; CPAC, 2012; CRTC, 2010c, 2013b, 2014f, p. 28; Linton, 2002; Sturgeon, 2012; Trichur, 2013). Often, these are calls for different classes of players (such as incumbents and their competitors) to be subject to the same regulatory treatment, but "leveling the playing field" can also justify regulatory discrimination to compensate for existing or potential imbalances.[164] If a player is perceived to have an advantage, then a level playing field can be

[164] Relatedly, "levelling the playing field" is also a way of talking about the need to overcome inequalities for Canadians living in different regions (CRTC, 2010c, 2014f, para. 6000), such as mandating services or rates for

achieved by imposing restrictions or requirements on that player, or compensating other players with special treatment (CRTC, 2005, para. 31, 2013b, para. 4383; Menzies, 2013).[165] This regulatory logic can be expressed through some unlikely pairings of metaphors, such as when the CRTC applied a "head start rule... to ensure a level playing field" (CRTC, 2006, para. 175).[166] Regulatory interventions are intended to better balance the relative positions of parties at the outset of competition, and once this is achieved, any subsequent inequality or advantage can be attributed to a player's superior competitiveness. But there has been no end to claims that the playing field of Canadian telecom is uneven, or that the game favors certain competitors, forcing regulators to constantly recalibrate the rules.[167] Of particular interest to this chapter is the notion that a level playing field can be created by mandating access to incumbent infrastructure.

It is important to remember that the state of play in Canada's telecom industry is directly descended from the relative position of the players in the early 1990s, following liberalization and at the start of the current era of competition. Previously, telephone companies had developed as 'natural monopolies' (Babe, 1990), often with generous government support,[168] including

incumbents serving rural areas.

[165] In Telecom Decision 2005-20, the CRTC created an incentive structure for telco incumbents (incumbent local exchange carriers, or ILECs) to provide a high quality of service for the smaller competitors that depend on using the incumbents' infrastructure. The incentives are meant to ensure that all competitors are treated equally by the incumbents (thus leveling the playing field between these competitors), as well as compensating for the power of the incumbents (leveling the playing field between incumbents and smaller competitors, see CRTC, 2005, para. 31).

[166] The ruling in CRTC Telecom Decision 2006-14 was intended as a fair way for smaller telcos to obtain broadcast licenses (as Broadcasting Distribution Undertakings, or BDUs), thereby allowing them to compete in the "core business" of cablecos. The CRTC decided that in exchange, the cablecos would require lowered "barriers to entry" to compete in the telcos' core business, which meant greater access to telco facilities.

[167] Most recently, the CRTC Chairman responded to a Bell representative's repeated calls for a level playing field by describing it as "elusive", and quoting a CRTC predecessor (David Colville) who "always mentioned that we're always looking for this level playing field", but even in sports the players must periodically switch sides (CRTC, 2016e, para. 2884).

[168] Some, like SaskTel, Manitoba Telephone System and Alberta Government Telephones were provincial crown corporations (SaskTel still is). Others (such as Bell) operated under government charters that granted them exclusive rights, in exchange for certain obligations (see Babe, 1990, p. 68).

guaranteed access to rights-of-way (Babe, 1990, p. 68; Martin, 1991, p. 23; Rideout, 2003, p. 19). Following privatization and liberalization, these telco incumbents enjoyed the advantage of owning vast communications networks in an industry that was now open to new entrants. The first cablecos developed in the 1950s through an uneasy dependence on the telco monopolies and leased access to telco infrastructure (Babe, 1975, 1990, pp. 215–216; Winseck, 1998, pp. 179–186). By the 1990s the cablecos owned infrastructure that had become largely separate from that of the telcos, with an effective monopoly on the last-mile of coaxial cable. Internet service could be provided over either cable or telco infrastructure, although cable offered an advantage in performance, and the extensive reach of Canada's cable companies helped make the country a leader in international broadband comparisons through the late 1990s and early 2000s (Frieden, 2005; Van Gorp & Middleton, 2010, p. 218). But new companies wishing to establish themselves as ISPs in the 1990s faced enormous challenges. The country was already wired by the telcos for universal phone service (which could be used to provide internet as DSL), and cablecos offered a superior alternative in urban areas. Without the ability to 'piggyback' on this existing infrastructure, new entrants would have to find a way to build expensive new networks from scratch before they could hope to attract any customers of their own. This was a 'barrier to entry' that new ISP upstarts could not surpass, thereby limiting competition to incumbents (generally, one telco and one cableco in any urban area), or to incumbents and new entrants that depended on access to incumbent infrastructure.

During the mid-1980s, Romaniuk and Janisch feared that, in the transition from monopoly-era regulation towards competition, Canadian public policy would be trapped in an unending “transitional period” of “regulated competition”. They warned of three dangers that accompanied such a halfway form of deregulation: “a sense of procreative responsibility [would] incline regulators to keep new entrants in business... an irresistible temptation [for regulators] to play the role of handicapper; and, third... opportunities created for strategic use of the regulatory process” (Romaniuk & Janisch, 1986, p. 612). Among ISPs, government's “procreative responsibility” has not been sufficient to prevent numerous smaller companies from being swallowed by incumbents.[169] However, a mandated wholesale access regime has been developed as a form of “handicapping” to compensate for incumbents' historic advantages. This regime sustains the surviving new entrants and imposes obligations on the incumbents that deal with them. Finally, regulating relationships between incumbents and IISPs has certainly led to “strategic use” of the regulatory process, wherein parties attempt to secure decisions that lower their costs and raise those of their competitors (Romaniuk & Janisch, 1986, p. 613).

While the CRTC is not the only federal agency that governs competition in Canadian telecom,[170] the regulatory regime it has created for this purpose is the most extensive and elaborate. Relationships between intermediaries are subject to different categories of CRTC-imposed obligations, advantages and disadvantages, depending on the parties involved. The public policy justifications for this regime have shifted over time, through different formulations of “facilities-based competition” and “telcom populism”, but the pursuit of a competitive market has remained central to its underlying logic. Ideally, competitive pressures should “discipline”[171]

[169] However, in recent years federal efforts have tried to forestall further consolidation in the wireless industry and to promote the viability of a national “fourth carrier”, including favorable terms for new entrants in spectrum auctions and government resistance to a full takeover of Mobilicity by one of the incumbents (Dobby, 2015d).

[170] Other agencies governing competitiveness in the telecom industry include Innovation, Science and Economic Development Canada (formerly Industry Canada), the Competition Bureau, and ultimately the federal Cabinet.

[171] For instance, competition restricts the ability to increase rates at will, producing “pricing discipline”. More broadly, “competitive discipline” refers to constraints on the ability of incumbents to dictate price and non-price components of service (CRTC, 2008, n. 3).

the behaviour of incumbents, leaving no room for abuses of market power.[172] However, these competitive pressures are often inadequate, and so the CRTC's regulatory regime has been required to impose discipline instead. The obligations of the regime therefore fall primarily upon the incumbents, who must provide wholesale access to their networks at regulated rates.

Who competes?

Before turning to the question of how competition is structured, or the obligations imposed through regulation-for-competition, I must clarify whether and how different classes of intermediaries are expected to compete. Canada's liberalized telecom regime is not one in which everyone competes with everyone else, and the majority of this chapter is devoted to discussing the obligations that incumbents have to cooperate with IISPs. But first it is important to reflect on the sorts of public intermediaries discussed in the previous chapter, whether these are municipal or regional ISPs, FreeNets, or RENs.

Since liberalization, the governing rationality has been that connectivity is best provided by competing private networks. Therefore, public intermediaries take steps to insulate themselves from the argument that they are somehow competing with private industry. They do so by serving the needs of a delimited public domain, such as public institutions (the MUSH sector),[173] by filling gaps neglected by private industry (CRTC, 2016c, paras. 16866–16891; Marlow, 2010), or by leasing capacity to private industry and claiming this supports a more

[172] Market power refers to the ability of a dominant firm to change prices or service without a competitive response. This is particularly the case where a single firm controls the market (owns the only facilities of a given type in a territory) and where “barriers to entry” prevent a competing firm to challenge this control by offering better prices or service.

[173] Examples include Axia's contractual separation of SuperNet functions, and RENs like CANARIE, BCNET and Cybera.

competitive market (Rick Adams & Coert, 2014; CRTC, 2014f, para. 7079). Even then, public connectivity projects are not immune from the criticism that they are competing with private business (Jackson, 2017b; Lie, 2003, p. 35; Wire Report, 2000b) or advantaging a government partner over other private companies (Massot, 2011; R. Shaw, 2012). As a result, it is important for public institutions to be able to claim that they do not compete, or that they act as enablers of competition on an equitable basis.

Originally, internet access was limited to publicly-funded research institutions, and to non-commercial uses as specified in acceptable use policies (AUPs). During the commercialization of the internet in the mid-1990s, these public institutions found themselves responding to demands for connectivity from various institutions, including private business (CA*net Institute, 2001, pp. 107–108). As private provision of internet access crystallized and incumbents began offering access, the internet gradually moved further from its public-sector roots, and RENs were left playing a limited role adjacent to the private market. For example, BCNET originally served a variety of public and private sector clients, before agreeing to restrict its scope and not compete with private ISPs.[174] By the 2000s, RENs had been limited to serving

[174] Before the mid-1990s, internet service could often only be obtained through an REN linked to CA*net. While the focus of these networks was research and education, BCNET ended up connecting a growing number of interested institutions, and Nova Scotia's network (NSTN) distinguished itself by taking a more commercial, for-profit route (CA*net Institute, 2001, p. 108; M. Hrybyk, personal communication, May 4, 2016). On March 31, 1997 CA*net “passed the torch... to the private sector” when the REN backbone was sold to Bell (CA*net Institute, 2001, p. 10). Some RENs were subsequently bought out by private industry (Lie, 2003, p. 8), while others had to change their focus. As BCNET's former President and CEO recounts: “At 2000 it was pretty clear that UBC needed world-class connectivity right, so they [all decided] to pony up... and make investments. And CANARIE put money in too, provincial government put some money in... so, we had to rededicate ourselves because we got provincial money to not being a commercial provider anymore. So that's in year 2000, we rewrote our mission statement saying we won't do that, we worked with the carriers and said... you know, how do we rewrite our acceptable use policy. If you look at it on our website, BCNET website, runs on for two pages, the reason is that they wanted to make absolutely sure we weren't competing with them” (M. Hrybyk, personal communication, May 4, 2016).

their traditional research and educational institutions,[175] leaving the market for residential and business clients to private industry.

While RENs were limiting their competition with private ISPs by focusing on a distinct set of users, some governments employed ISPs as instruments of connectivity for a larger public. When they established their own networks, governments often sought to avoid competing with private industry for the same clients. When governments enrolled private industry to serve public policy, they had to answer claims that they were unjustly favoring certain private partners. The solution in both cases is often some version of an 'open-access' approach, which mandates access to infrastructure for competing intermediaries. For example, as discussed in the previous chapter, a number of cities in Western Canada have constructed their own dark fibre networks in recent years. Public ownership in these cases is aligned with the rationality of liberalization by making municipal networks available to private industry, sometimes accompanied by the suggestion that this would actually increase competition (City of Calgary, 2014a, para. 7079). Where the network remains in the hands of a private company under a public mandate, its operation is often subject to rules regarding competition. The terms of the BC government's agreement with TELUS (Connecting British Columbia Agreement, 2011), and Axia's contract with the Alberta government (Government of Alberta et al., 2005) both restrict the ability of these companies to use government-funded facilities for their competitive advantage.[176] In these cases (and others, see EORN, n.d.; SWIFT, 2016), funding to extend rural connectivity is accompanied by the goal of promoting rural competition, and this should not result in a competitive advantage for any

[175] As discussed in the previous chapter, some RENs also serve innovation and entrepreneurship-enabling functions, but these efforts must be carefully directed to avoid competing with private industry (R. Winsor, personal communication, June 16, 2014).

[176] Axia has been quite successful in working around these restrictions in Alberta. See Chapter 2.

private sector partner.

When a private company operates infrastructure under a public mandate, rules such as those listed above can amount to telling a private company not to compete in certain ways. As the price of benefiting from a public mandate, ISPs can be compelled to serve their competitors, or to avoid behaving as a competitor in a particular market. A role conflict develops when a company is expected to maximize the value of a network's points of control against its competitors, while simultaneously being obliged not to compete. This can result in controversies similar to those between incumbents and IISPs discussed later in this chapter, as private companies look for ways to profit while adhering to their formal obligations. However, the potential for this role conflict depends on a particular view of how competition in telecom should operate. Specifically, it is based on the notion that control over telecom 'facilities' should be a source of competitive advantage, rather than competition (in 'services') over a shared infrastructure governed toward maximizing public benefit.

Facilities-based competition

The public policy objective examined in this chapter is competition or ‘competitiveness’, but these terms have several distinct meanings which lead to very different governing rationales. For instance, competitiveness might refer to the number of competitors in a market, or the extent to which companies offering similar services compete. Competitiveness can also be interpreted as some form of efficiency, for which a monopoly or duopoly are arguably well-suited (Davies, 2014, pp. 91–92). And finally, there is 'national competitiveness', in which nations are seen as competing with one another for economic prosperity (Davies, 2014, Chapter 4; for example see

Industry Canada, 1994, pp. 4–5; Janisch & Schultz, 1991). When it comes to governing the various components that constitute the internet, there is also the question of *where* competition is desirable. Is it in the public interest to have competing networks, with multiple sets of wires running above and under public roads, or would it be better to have multiple internet services available over a common physical infrastructure? The last of the above-mentioned distinctions is typically known as the debate between facilities-based or service[s]-based competition. Public policy can either try to promote competition in facilities (the material infrastructure of networks) or services (offered over a shared material infrastructure).

In Canada, while the federal government has officially promoted facilities-based competition since the mid-1990s, the advantages of sharing infrastructure have also been recognized as a way to promote a number of public policy objectives, including efficiency and national competitiveness.[177] In specifying federal telecom policy, the CRTC has alternated between insisting on the long-term guiding principle of facilities-based competition, and recognizing that not all facilities can or should exist as multiple, overlapping sets. The CRTC has largely avoided the question of what an "ideal" (CRTC, 2015e, para. 5) world of facilities-based competition would look like (how many competing infrastructures should exist, of what kinds, and in which geographical areas).[178] Instead, the tendency has been to look at the industry for indications of competition and market power, to find not enough of the former and too much of

[177] Examples of other public policy objectives served by shared telecom infrastructure include a reduced impact on public rights-of-way (such as the inconvenience caused each time a service provider must access its infrastructure buried under a roadway), and the desirability of less-visible infrastructure (such as fewer cell towers) as an aesthetic preference expressed by local residents (City of Calgary, 2014b; Federation of Canadian Municipalities, 2009).

[178] The exception here is the wireless market, where the goal of four national carriers (the three incumbents – Rogers, TELUS and Bell, plus either a new national player, or at least one additional competitor in each market) was explicitly pursued by the Harper Government beginning in 2012, in large part through rules governing spectrum auctions (Geist, 2014c; Kyonka & Doyle, 2012; Trichur, Silcoff, & Erman, 2013).

the latter, and for the CRTC to prescribe mandated access to infrastructure as a solution.

As described in Chapter 1, telecom liberalization took place gradually in Canada, picking up steam in the 1980s, but with a great deal of uncertainty over the parameters of a newly competitive market. In the general considerations for its decision on whether to allow competition in long-distance telephone service (CRTC, 1985), the CRTC (1985) noted that while its mandate did not favor either competition or monopoly in any specific telecom service, it was certainly open to the argument that the duplication of facilities ran counter to the public interest.[179] When the same issue came before the CRTC in 1992 (CRTC, 1992), the Commission came down solidly on the side of promoting competition, opening the long-distance market to facilities-based competition as well as "resale" (allowing new entrants to "resell" long-distance service through incumbent facilities at a [potentially] lower price). However, while the CRTC saw many benefits for allowing new entrants to resell incumbent services (including disciplining marketplace behaviour), it argued that this was "not a substitute for facilities-based entry", which "permits sustainable and more broadly-based competition" (CRTC, 1992, sec. C.1). For Winseck, the difference between the 1985 and 1992 long-distance decisions demonstrates how competition had "achieved ideological status within the CRTC" and become an "end in itself" (1998, p. 247). The Commission did not have long to wait before federal legislation gave added support for its "new religion" (Winseck, 1998, p. 248) of promoting competition, although it would be several more years until the rationality of facilities-based competition was clearly articulated and accepted.

The *Telecommunications Act* of 1993 set out several broad objectives for telecom policy

[179] The Department of Communications also voiced concerns about the duplication of facilities as late as 1988 (Babe, 1990, p. 240).

in Canada, as entrusted primarily to the CRTC. These policy objectives include enhancing "the efficiency and competitiveness, at the national and international levels, of Canadian telecommunications" and "increased reliance on market forces for the provision of telecommunications services" (Government of Canada, 1993, sec. 7). However, this said little about exactly what competitiveness entailed, how efficiency and competitiveness were to be determined,[180] and where regulation was to give way to market forces. The importance of greater competition in telecom facilities, products and services was affirmed through the mid-1990s in a number of government studies (CRTC, 1995; Information Highway Advisory Council, 1995, 1997), an action plan (Information Highway Advisory Council, 1996), policies (Government of Canada, 1996) and telecom decisions (CRTC, 1994).

Greater specificity eventually came through an important 1997 decision,[181] in which the CRTC stated that "the full benefits of competition can only be realized with facilities-based competition" (CRTC, 1997, sec. 237). In the Commission's view, "efficient and effective competition" was best pursued through competing infrastructure - separate cables, wireless antennas, cabinets and routers. Otherwise, competition might be cultivated at the retail level (through mandated wholesale access to incumbent networks), but incumbents would retain a

[180] Regulatory arguments over mandated access often present competing ideas about efficiency and competition. As a number of parties advocating for mandated access to fibre networks argued, duplicate (competing) facilities, such as multiple fibre lines to the same destination, are an inefficient use of resources and investment capital. A world with multiple last-mile fibre lines is one in which some of these lines go unused or lie "fallow" (CRTC, 2014c). To argue the opposite position, Bell has put forward the view that "Facilities based competition is much more beneficial to economic efficiency than is resale competition [mandated access]... [because] facilities based competition creates important dynamic economic efficiencies as carriers compete to lower their costs so they can lower their prices" (Bell, 2015, p. 39).

[181] CRTC 97-9 gave new entrants (Competitive Local Exchange Carriers, or CLECs) wholesale access to the copper networks of incumbent telcos (Incumbent Local Exchange Carriers, or ILECs, see Van Gorp & Middleton, 2010, p. 221). This was a direct consequence of Telecom Decision 94-19 (CRTC, 1994), and came shortly after the Convergence Policy Statement (Government of Canada, 1996), which stated that "facilities and capacity of telecommunications carriers... be made available for lease, resale and sharing by service providers and other carriers on a non-discriminatory basis".

wholesale monopoly (CRTC, 1997, sec. 73). The supposed gains of competition: increased investment, innovation, and efficiency (with resulting price reductions), needed to be realized at the level of facilities, where they would have the greatest impact.

As the rationality of facilities-based competition became regulatory common-sense in Canada, it translated to the notion that “real competition... is only possible with a separate wire into the house” (T. Denton, personal communication, November 12, 2014). This was even as other countries (particularly in Europe) were following a different course of liberalization that depended on mandated wholesale and leased access to telco infrastructure. This European approach (known as service-based competition) “was treated as if it were irrelevant” by Canadian regulators, because Canada had a well-developed cableco infrastructure to compete with telcos (Denton, 2013).[182] Finally, facilities-based competition was preferable to mandated wholesale because mandated access requires more regulation.[183] In a mandated wholesale regime, the prices charged for access to facilities need to be regulated, which places the regulator (the CRTC) in the difficult role of determining incumbents' costs of operation (Denton, 2013). Mandated wholesale would keep the CRTC engaged in setting rates, forestalling further deregulation and the transition to market forces.

The reasoning that telecom policy should be oriented towards promoting facilities-based competition was hardly unique to Canada in this period (Frieden, 2005; Paltridge, 1995; Woroch, 1998). Most notably, facilities-based competition was also being promoted in the US. While

[182] Internationally, Canada is unusual in the reach of its cable network and because its regulatory regime mandating wholesale access to bath telco and cableco infrastructure (Van Gorp & Middleton, 2010, pp. 220–221).

[183] Regulation and competition are also often understood to be opposites, so that “If you’re gonna have leased-based access, you’re gonna have more regulation. End of story. And if you’re gonna have more regulation that looks like, less competition” (T. Denton, personal communication, November 12, 2014).

Canadian liberalization deviated from the US model in some important respects,[184] Canadian regulators were certainly aware that liberalization was taking place in a continental context, and the policy regimes of both countries shared some fundamental assumptions and methods (K. G. Wilson, 2000).

In Canada, the facilities-based orientation of competition was emphasized through CRTC decisions into the 2000s (see CRTC, 2002) and reached its high-water mark in the Minister of Industry's 2006 policy direction (Government of Canada, 2006).[185] The policy direction was a remarkable and unprecedented statement intended "to remind [the CRTC] that Canada is a capitalist country, a country of freedom, and that regulation must be as limited as possible, to allow market forces to play out" (Standing Committee on Industry, Science and Technology, 2006). But even as the Conservative government committed the CRTC to reduce regulation and govern through market forces, regulatory decisions were extending and solidifying a regime of mandated wholesale access through incumbent facilities. In other words, despite a commitment to foster the "construction of competing telecommunications network facilities" (Government of Canada, 2006), regulators were extending obligations to share facilities. Much of the rest of this chapter is devoted to explaining this apparent contradiction.

Mandating wholesale

Wholesale access to some telco facilities was mandated in the very same CRTC decision

[184] Particularly in resolving questions of jurisdiction over telecom and in a greater tolerance for vertical integration in Canada (K. G. Wilson, 2000, p. 276).

[185] Specifically, the policy direction stated that CRTC should act "with a view to increasing incentives for innovation and investment in and construction of competing telecommunications network facilities" and to review "mandated access to wholesale services, to determine the extent to which mandated access to wholesale services that are not essential services should be phased out" (Government of Canada, 2006). The policy direction's embrace of market forces would also shape the *Spectrum Policy Framework* for wireless connectivity (Industry Canada, 2007).

that affirmed the importance of facilities-based competition (CRTC, 1997), and this obligation was subsequently extended “until such time as the market for such facilities is sufficiently competitive” (CRTC, 2001). While presented as a “transitional” approach (CRTC, 2002, sec. 26) that would allow new market entrants climb the “ladder of investment”[186] to owning their own facilities (Cave, 2006; Van Gorp & Middleton, 2010, p. 220), mandated wholesale access to incumbent networks became an enduring feature of Canadian telecom regulation. A series of “micro-regimes” (Levi-Faur, 1999) were developed to mandate access and to set tariffed rates for specific networking infrastructures and technologies. Beginning with telco facilities in 1997, mandated access was extended to cablecos in 1999 (CRTC, 1999), following (and followed by) years of resistance to these obligations by the cable industry (Menard & Denton, 1999; Van Gorp & Middleton, 2010, p. 221). Most recently, mandated access has been extended to FTTP, and the resulting regulatory conflict has even drawn in municipal leaders (Geist, 2016a).

Incumbents with massive investments in facilities frequently disagree with the mandated wholesale regime. They argue in favor of facilities-based competition, and emphasize the Canadian market is already highly competitive with some of the best networks in the world (CPAC, 2010, 2011, 2012, 2013a, 2014; CRTC, 2014b; Rajabiun & Middleton, 2015, p. 49). According to incumbent voices, supporting smaller competitors thorough mandated wholesale is an “artificial” form of competition (Dobby, 2014c), that “distorts” the market (ISP Summit, 2013) or replaces competition with “regulated arbitrage” (CPAC, 2014). A common criticism of the mandated wholesale access regime is that it gives new entrants little reason to build their own facilities, since they can make use of incumbent networks, thereby undermining the ladder-of-investment theory (Beaudry, 2010; CPAC, 2014; CRTC, 2014b; Telecommunications Policy

[186] An often-used alternative metaphor involves stepping stones instead of a ladder.

Review Panel, 2006, Chapter 3).[187] But the CRTC has continued towards its stated objective of facilities-based competition by forcing incumbents to share their networks with competitors, thereby supporting the viability of intermediaries that are incapable of competing on the basis of facilities.

The contradictions of this policy have previously been resolved by combining the rationality of facilities-based condition with ideas such as the ladder of investment and the pursuit of the level playing field. Since competitors are not equal at the outset (with incumbents benefiting from the legacy of the monopoly era), new entrants need some regulatory advantages to be competitive and to invest in their own facilities. One problem has been that actors in the policy debate disagree on what would make the playing field even. Another is that government and regulators have never clearly defined what the desired future of facilities-based competition looks like. This means that while the rationality of facilities-based competition has been clearly articulated (stating that competing facilities are the best way to increase the competitiveness of the industry), it is impossible to know at what point the market in facilities will be sufficiently competitive.

Facilities-based competition is still cited as a rationale for CRTC decisions, but it has become a hypothetical long-term end state, to be achieved when the market for facilities is competitive enough (see CRTC, 2011c, para. 5378). The criteria for achieving this condition of competitiveness have been left unstated, but the clear implication of government decisions (including those of the CRTC and Cabinet) is that abandoning mandated wholesale would result

[187] A related criticism of the ladder-of-investment theory, but one which argues in favor of wholesale access, is that not all service providers want to be facilities-based, and there are good reasons why some would want to focus on services (CRTC, 2014b, paras. 4738–4748; T. Denton, personal communication, November 12, 2014; Denton, 2014b).

in something short of the goal. Deregulated facilities-based competition can only begin when the playing field is leveled and the advantages of incumbency are neutralized. Incumbents' responsibility to provide wholesale access is justified as an important leveling technique, despite the fact that the constant extension of this responsibility demonstrates just how ineffective it has been at erasing the advantages it is meant to address.

The mandated wholesale regime has contributed to the "legal potential" for competition (Winseck, 1998, p. 272) rather than creating new facilities-based competitors.[188] While in theory, Canada's liberalized regulatory regime allows new players to enter the market and compete, in practice the 'barriers to entry' have meant that any new entrant would have to invest billions of dollars to build facilities comparable to the incumbents.[189] These high barriers to entry, resulting in inadequate levels of competition, are referred to by economists as a form of "market failure" (Crouch, 2011; Gómez-Barroso & Feijóo, 2010), with incumbents maintaining considerable market power over new entrants (CRTC, 2015e).[190] The mandated wholesale regime is meant to address abuses of market power, but it has created a fundamental role conflict for the incumbents it obliges to both compete and cooperate. IISPs meanwhile, are reliant on companies that often compete with them for the same customers, and the CRTC is left adjudicating the resulting

[188] Winseck argued in the mid-1990s (1998, p. 272) "that when the CRTC speaks about competition, it does not mean real competition but only the legal potential for it". On this basis, regulation has effectively created a potential for competition. However, there are indications that the failure to produce "real competition" through the previous facilities-based approach has been recognized as a problem the CRTC (Denton, 2013).

[189] The only real potential for such a well-resourced competitor has come from abroad, but foreign ownership restrictions have long made this impossible or difficult. The last time a sizable foreign firm seriously considered entering the Canadian market was in 2013, when Verizon apparently entertained the notion of bidding for wireless licenses. Verizon's entry was vigorously opposed by Canadian incumbents, arguing that the "massive incumbent U.S. carrier" would receive "favourable treatment" as a new competitor and create an imbalanced playing field (Bell, Rogers, & TELUS, 2013a; Trichur, 2013).

[190] The terms "market failure" and "market power" (and whether these states accurately describe the industry) are highly contentious in Canadian telecom. IISPs often point to the market power of incumbents, while incumbents tend to minimize their own power by emphasizing the competitiveness of the existing market (CPAC, 2011, 2013a; CRTC, 2015e).

disputes.

Competitive dependency

To summarize the developments detailed above: Competition became a guiding principle of Canadian telecom regulation in the 1990s, supplanting the previous arrangement of regionally-based telco and cableco monopolies. Facilities-based competition was the governing rationality, and this meant encouraging the construction of competing telecom facilities. It was imagined that facilities-based competition could be achieved by compelling incumbents to make their infrastructure available for use by their competitors. This would allow 'new entrants' to the telecom industry to grow their businesses and invest in their own facilities, until they were no longer dependent on the incumbents. Incumbents would be forced to adopt a number of responsibilities in regard to their smaller competitors. They would have to coordinate customer ordering and installation, billing, troubleshooting and the physical interconnection of equipment with these new entrants. The regulator (CRTC) would set tariffed rates for access to incumbent networks, and review these relationships over time to see if they were still necessary. Once the consumer market was sufficiently competitive (a threshold which was never defined), regulated access to incumbent networks would be ‘forborne’, or lifted. The regime of wholesale access to incumbent infrastructure would be a transitory form of regulation until the imbalances inherited from the monopoly era had been corrected.

But the legacies of the monopoly era would not be so easily amended. New entrants found the road to facilities-based competition to be either undesirable or impassable. Tariffed wholesale rates did not allow IISPs much room to compete by offering lower prices than incumbents or to fund the infrastructure to successfully decouple from incumbent networks. IISPs were more concerned with covering their expenses than raising billions of dollars to duplicate incumbent facilities. Many local and regional companies were satisfied with their limited footprint, and had no ambition to grow into carriers. As a result, the temporary wholesale regime that allowed competitors to climb onto incumbent networks became more durable, and regulatory conflicts gradually settled into contests over the details of these arrangements (such as costing).

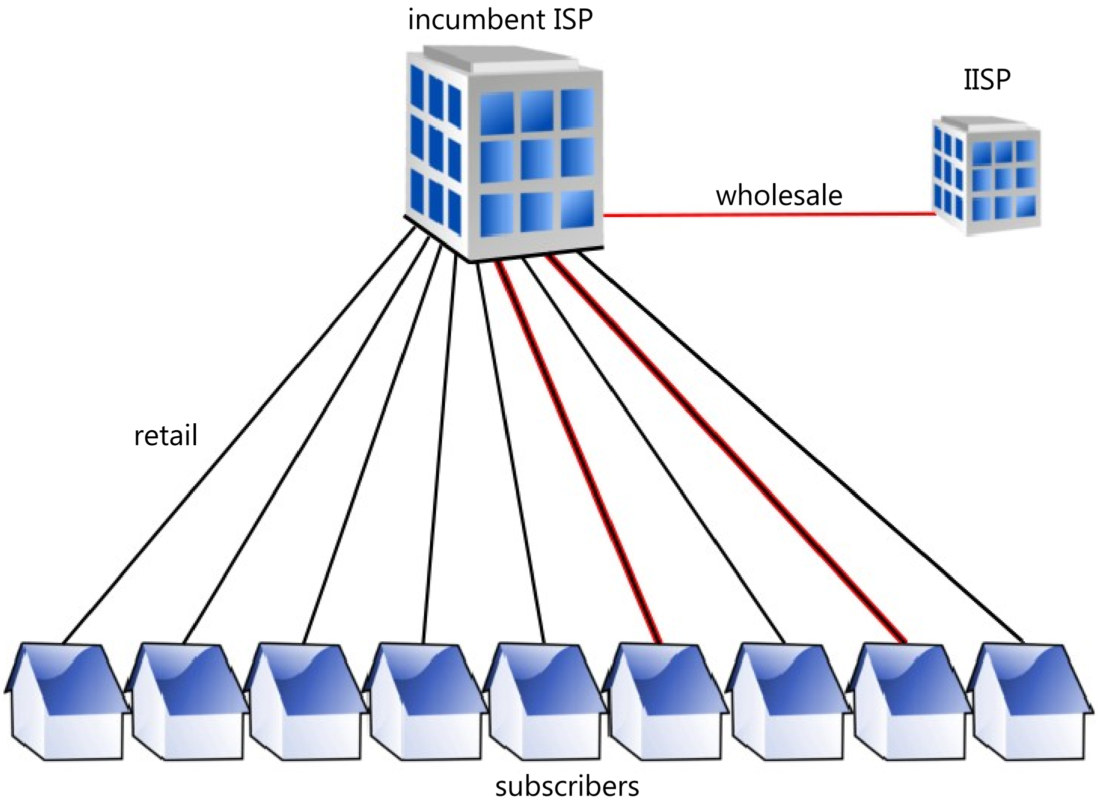
These developments have resulted in a state I will describe as competitive dependency, in which dependencies exist between competitors, and wherein competitors are expected to cooperate. Competitive dependency exists where power relationships between competitors are highly unequal, and regulators extend obligations from the most powerful (the incumbents) to the least (the IISPs). In Canadian telecom, this enduring arrangement came with a host of responsibilities for incumbents, who were compelled to support to their unwanted dependents, with the CRTC acting as a referee.

IISPs are sometimes characterized as being a burden for incumbents, who “do not earn a compensatory return on [their] network investments from these customers” (CRTC, 2014g). While not unprofitable (CRTC, 2015f), wholesale customers are less profitable than an incumbent's own retail customers.[191] However, the tension created through the obligation to serve a less-desired class of customers is not as fundamental as the role conflict underlying the mandated wholesale regime. This role conflict, which imposes contradictory expectations of behaviour on incumbents, results from the fact that IISPs are both wholesale customers and retail

[191] This led Rogers to recently argue that retail customers were “subsidizing” wholesale customers, partly because wholesale customers have been responsible for a growing share of the demand on Rogers' network (CRTC, 2014g).

competitors. As wholesale customers, IISPs bring considerable revenue to incumbents and must be served according to CRTC regulations. As competitors, IISPs attract subscribers who might otherwise pay an incumbent even more as retail customers,[192] and the regulatory regime presumes that incumbents and IISPs will compete with one another for these customers.

Figure 2: Competitive Dependency



IISPs are served by an incumbent's wholesale division, which is dedicated to treating them as clients and addressing their needs. Wholesale account executives sell internet access to IISPs and manage these relationships, sometimes competing with other wholesale access

[192] Even in an area where an incumbent has neglected last-mile services, as in parts of rural Canada where retail customers are not as profitable, small IISPs built to serve local needs can be seen as competitors for future opportunities – when the incumbent feels the area is worth investing in.

providers who serve the same area.[193] Other employees maintain the interconnections between incumbent and IISP equipment, and troubleshoot technical problems experienced by the IISPs. Some countries have pursued "functional separation" of incumbents' wholesale and retail divisions to promote competition (OECD, 2012), but in Canada no such requirement exists (Middleton, 2011).[194] Therefore, incumbent wholesale divisions vary in how independent, resourced and driven they are to compete for new business.[195] Conflict arises when the goals of wholesale and retail work against one another, or wholesale becomes subordinate to retail, since a growing number of well-served wholesale customers are likely to result in fewer retail customers. In the end (at the literal end of the network, or the bottom of Figure 2), retail and wholesale serve the same customers. However, retail serves these end-consumers more directly and profitably, while wholesale does so through another intermediary that can be seen as a retail competitor.

Because retail tends to be more profitable than wholesale, and IISPs depend on incumbents for wholesale, there is always the danger that this wholesale dependency will be used against IISPs by incumbents in order to compete for the same individual subscribers. The inequalities and dependencies between these two categories of intermediaries give incumbents various advantages and points of leverage. First, incumbents can simply choose to neglect their

[193] While some incumbents might prefer not to serve IISPs, given the existence of mandated wholesale, incumbents sometimes compete with one another for these customers by lowering rates below what they are obliged to charge (CRTC, 2014g, paras. 8794–8824).

[194] However, there is a requirement for wholesale providers to isolate wholesale customer information from their retail operations through an internal carrier services group (CSG, see CRTC, 2011d). This is meant to prevent incumbents from trying to retain or reclaim retail customers who have transferred to an IISP being served through an incumbent's wholesale division.

[195] According to the Chief Legal and Regulatory Officer for TekSavvy, an IISP served by six different incumbent wholesale providers (TekSavvy, 2016), there are significant differences in how these companies treat their wholesale customers due to "organizational culture and resource allocation", such as "how well a [carrier services group] is staffed or what resources it has, especially in terms of systems" (B. Abramson, personal communication, January 27, 2017).

wholesale business, providing service but only doing the bare minimum to meet their regulatory obligations.[196] Secondly, incumbents can actively exercise market power against competitors, exploiting their control over "upstream" or "bottleneck" facilities to control competitors' rates (CRTC, 2015d), service (CRTC, 2010a), or behaviour (CRTC, 2014a; Henderson & Karadeglija, 2014). Thirdly, incumbents provide the information used as a foundation for CRTC decision-making, namely through cost studies. These document incumbent costs for providing services, are submitted in confidence, and are used by the CRTC to set "just and reasonable" wholesale rates. While the CRTC can disagree with incumbents' cost studies (CRTC, 2016d), it is up to IISPs to challenge any rates approved by the Commission which may be unfair or result from "costing error" by incumbents (see CRTC, 2013a).[197]

It is the CRTC's sovereign responsibility to determine what kinds of obstacles imposed by incumbents against wholesale access should be considered undue discrimination, and so the Commission adjudicates a never-ending "tug of war" (Van Gorp & Middleton, 2010, p. 222)

[196] One wholesale customer described the local telco incumbent's attitude towards mandated wholesale as, "Well, they made us do this, that doesn't mean we have to provide it well, you know, or provide you with good service, or any of that stuff. So technically they're meeting, you know, all of the requirements right, but in practical terms they're not" (N. Ouzas, personal communication, October 8, 2014). This type of neglect is less likely when two incumbents compete in the same territory, since either incumbent can choose to provide more attractive wholesale service to gain clients at the expense of the other (as happened between Bell and Cogeco in Ontario, see note 201 below).

[197] As George Burger of Vmedia argues, "We're in a framework where... clearly we have our respective roles... the incumbent's role is to keep complaining about the fact that [IISPs] keep bringing up rates, and the [IISPs'] role is to keep examining rates and trying to get to some truth of it. The difference between the two of us, or our two sides, is that only one side really has the truth of what these things, these underlying things cost. And as part of the role of that side, their role is to try to game the presentation of that truth as much as possible in the process" (CPAC, 2015). However, the truth of costing is hardly transparent in a world where transmitted data packets have almost no marginal cost and incumbents' spending is primarily through investment in infrastructure (see CRTC, 2014b, pp. 3762–3770). Ultimately, it is up to the CRTC to evaluate cost studies and determine the truth of the matter. Ken Engelhart of Rogers (CPAC, 2013a) has criticized this process as "a bit of a dark art" which can result in some baffling CRTC judgments (citing an example in which a Cogeco network adjacent to Rogers was costed at twice the rate). Englehart also criticizes how the regulatory regime rewards those who work it most effectively, stating: "I don't think costing can ever be good enough or accurate enough to really sustain a competitive system like this. The whole system depends, not on how good your sales is, not on how good your marketing is, not on how good your engineering is, but how good your costing people are" (CPAC, 2013a).

between incumbents seeking to restrict wholesale access to their networks, while IISPs seek to extend access. Regulatory inequalities between incumbents and IISPs are put on public display at CRTC hearings, where incumbents sometimes appear before the Commission with large panels of lawyers, executives, and experts, while IISPs more typically pool their resources for regulatory affairs. In a regulatory process that is meant to protect them from the worst effects of dependency, IISPs are at a disadvantage in terms of resources and participation.[198]

As one example of how competitive dependency operates in practice, IISPs rely on incumbent last-mile infrastructure, and so it is the incumbent's responsibility to sends a technician to service an IISP subscriber's home. In 2013, IISPs (represented through CNOC) alleged that cablecos were unduly discriminating against them by making wholesale access difficult to obtain and providing inferior service to retail customers (Kyonka, 2013a). TekSavvy's subscribers experienced long disruptions of service that the IISP was unable to resolve on its own, and one group of customers reported that their problems were quickly corrected once they switched to become customers of the incumbent (CBC News, 2013). Ultimately, the CRTC ruled that IISPs failed to demonstrate that they were being discriminated against, because they lacked a way to contrast their treatment with the treatment of the cablecos' retail customers (CRTC, 2015b, para. 17). This highlights the informational asymmetry between IISPs and incumbents,

[198] During the CRTC's wholesale service review in 2014, the CRTC Chairman joked about the Bell representatives (numbering fourteen) "testing the capacity of our witness tables" (CRTC, 2014d, para. 2931). By pooling resources, IISPs represented by CNOC (currently the most important organization representing IISPs' regulatory interests, primarily through legal counsel Chris Tacit, see *Who we are, what we do, and why you should be a part of it*, 2013) can also appear in significant number, including CEOs and Presidents of several companies, along with lawyers and experts (see CRTC, 2014c). Incumbents may have greater resources, but the size of an organization's regulatory department does not always carry the day before the Commission, where minor actors have sometimes had their complaints upheld against the largest of incumbents (CRTC, 2015a; Roseman, 2012). However, simply participating in CRTC proceedings can be a significant hurdle (Rajabiun & Middleton, 2015, p. 40), and most IISPs are not CNOC members.

since only the cablecos are in a position to provide such a comparison to the CRTC.[199] The Commission ordered both groups to discuss and resolve their issues, and this is just one example of the many disputes that have arisen between incumbents and IISPs (Middleton, 2011, pp. 65–66), due to the expectation for incumbents to treat IISPs as both competitors and customers (Middleton, 2011, p. 65).

Incumbents vary in how they choose to navigate this service provider/competitor role conflict. At events such as the ISP Summit and BCBA Conference (both of which cater to IISPs), some incumbents act as sponsors and try to attract wholesale customers, while others are conspicuously absent. Discussions at these events often lead to comparisons of how different incumbents manage their wholesale relationships. Relationships with incumbent wholesale providers can also change over time, including a trend in which IISPs have increasingly been treated as valued wholesale customers (rather than burdens or competitors).[200] This is a shift that has taken place at a number of incumbents who have come to terms with the permanence of the wholesale regime and the sustainability of IISPs, with competition for wholesale business becoming so important that these relationships cannot simply be ignored in favor of retail

[199] According to TekSavvy’s Chief Legal and Regulatory Officer, the most important advantage incumbents have (in addition to greater regulatory resources) “is that when it comes to wholesale, it’s their network, not ours. They have an inside view that we do not – on what is possible or not, what works or not, what costs what, and so forth” (B. Abramson, personal communication, January 27, 2017).

[200] An Edmonton-based IISP President described the wholesale division of the local telco incumbent as previously being “the ass-end of TELUS. They sent people in TELUS to that division to go and piss off guys like me... [they] were unpleasant to deal with, hated us, didn’t want to have meetings with us... anytime that you asked for something it was 'no'”. Then, after 2011, a change occurred which he attributed to the creation of CNOC, more assertive IISPs, wholesale competition between incumbents, and a “generational shift” within TELUS. As a result, TELUS “completely revamped their attitude. They’re now asking us to sell more services. They’re busy trying to figure how to bring prices down. They’re trying to help us increase business with them. It’s 180 degree turn... what these guys have done is said... our customers are not our competitors” (G. Fletcher, personal communication, July 20, 2013). Elsewhere in Alberta, Olds’ O-NET maintains a good relationship with Shaw’s wholesale division as a customer purchasing connectivity to YYCIX in Calgary, while competing against Shaw’s retail division within the town itself (Gustafson & McInnis, 2016).

customers.[201]

While the wholesale access regime does impose some clearly-defined obligations on incumbents, it does not constrain incumbent-IISP relationships into a rigid mold, and incumbents maintain a great deal of discretion in how they approach their wholesale relationships (B. Abramson, personal communication, January 27, 2017). One indication of a more cooperative relationship between incumbents and IISPs are "off-tariff" deals, with prices and terms agreed-upon by both parties rather than according to CRTC mandate (CRTC, 2013c, 2015c, p. 262). Incumbents point to these deals as evidence of vigorous wholesale competition (CRTC, 2014d), and have sometimes claimed that they would continue to provide wholesale services on negotiated terms even without a mandated wholesale regime (ISP Summit, 2013). However, these off-tariff deals presume that the wholesale regulatory regime looms in the background as a regulatory "backstop" (CRTC, 2014g), and IISPs rightly fear that without a mandated set of obligations, their ability to negotiate for agreeable terms would be greatly reduced (CRTC, 2014c).

In summary, competitive dependency in Canadian telecom arises from highly unequal power relationships, and the disciplining of incumbent behaviour by the mandated wholesale regime. The resulting condition is one in which IISPs are protected from total dominance by

[201] As Bell's Mirko Bibic recently explained before the CRTC: "We were losing share to cable TPIA [wholesale]. What did we do? We didn't just hang back and say: This is wonderful. Our tariffed rates aren't satisfactory to our customers. Great, now we don't have to deal with wholesale anymore. It's nirvana. No... With the ability to do off-tariff deals we have struck arrangements with ISPs to encourage them to come back. And why is that? The reason is simple. We are investing and we are competing so hard at retail there is inevitably a retail loser in the market share game. And it shifts over time. That loser wants to fill the pipe and is trying to regain losses at wholesale. The other one is saying, 'I'm losing my wholesale share now. I have to -- forget what my tariff says, I want to go compete'. So we did off-tariffed deals" (CRTC, 2014d, paras. 3471–3474). Likewise (and in competition with Bell) Cogeco has also pursued "improved cooperative business relationships" (CRTC, 2014e, para. 4609) with IISPs, including lowering rates. Off-tariff deals have also reportedly become more common in British Columbia (CRTC, 2014c, para. 2807).

incumbents, and which obliges incumbents to serve IISPs. However, in the interest of promoting competitiveness, the regime violates the most important rule in competition: that contestants not cooperate with one another (Davies, 2014, p. 41). Role conflict regularly occurs as incumbents are expected to both compete and cooperate with IISPs. The following section will examine why this regime has endured, despite the tensions it produces and its failures in producing new sources of facilities-based competition.

Accounting for the mandated access regime

Given that the efforts of the CRTC and successive federal governments to foster telecom competition have stretched on without end, we can conclude that the telecom market has failed to develop in a way that meets public policy expectations. This raises the question of what has sustained a regulatory regime that has been so inadequate at achieving its stated objectives. As previously discussed, incumbents have argued that vigorous competition can (and does) exist between a small number of giant firms,[202] but this argument has not persuaded Canadian governments to abandon regulation-for-competition. The continuation of mandated wholesale has become a way of forestalling a broader form of market failure that would lead to the collapse of smaller competitors and further industry consolidation.

Several factors account for the extension of mandated wholesale, and will be described below. First, mandated wholesale continues because incumbents still have market power, which they would presumably exploit if incumbent wholesale obligations were removed. The fact that the regime has been ineffective in eliminating this market power has not been taken as a reason

[202] Three firms are considered a sufficient number, according to the Chicago school of economics (Crouch, 2011, p. 60).

to abandon the regime (which would mean accepting incumbent dominance) or as reason to pursue more comprehensive forms of mandated wholesale (through services-based competition and structural separation), and so the existing approach carries on as a sort of middle road. Secondly, increasing consumer choice has been a way for the federal government to cater to populist sentiment, and since 2011 mandated wholesale has been seen as an issue that can attract significant public interest. Finally and most recently, it appears that the objectives of mandated wholesale are no longer as stated in the 1990s. In fact, the regime can even be considered successful as a result of goal-shifting, thereby justifying its continuation.

The middle course and the triumph of the giant firm

Incumbent dominance after liberalization can be partly explained by specific features of the telecom industry, such as high barriers to entry for facilities-based providers, but it is also consistent with outcomes in other industries where neoliberal rationality has supposedly prevailed. As Colin Crouch (2011) argues, neoliberal policies like privatization and liberalization do not tend to create the competitive markets that justify them, but instead favor dominance by giant firms (often the same corporate actors supporting neoliberal policies). This forces us to consider whether "the virtues of the market [are] better expressed in the maintenance of competition, and therefore with the existence of large numbers of competing firms, as in pure economic theory, or in the outcome of competition, which may often mean the survival of a few giant corporations and diminished consumer choice" (Crouch, 2011, p. 53). In other words, should a market-based approach support a large number of competitors, or should we accept the continued dominance of Canada's telecom industry by incumbents as the predictable result of competition? Successive governments' support for regulatory capitalism through mandated wholesale indicates a desire for more competitors and an unwillingness to cede the field to incumbent 'survivors'. But this has also been the limit of regulatory intervention, since the idea of a transition to service-based competition contradicts the dominant facilities-based rationality, and has remained at the margins of political possibility. Mandated wholesale is a path between a pure form of facilities-based competition and a full commitment to shared facilities, because either turn would have consequences that are deemed unacceptable.

To turn away from a mandated wholesale regime and toward closed, competing facilities would mean openly accepting the incumbent-dominated status quo that competition was meant to unsettle. Deregulation of wholesale seems to await a time when doing away with the regime will not result in the downfall of IISPs and the survival of the incumbents. By this logic, we can only know the outcome of facilities-based telecom competition once there are a large number of truly competing firms. Despite the opening created by liberalization, these conditions are no closer to being realized now than they were a decade ago, because intermediaries utilizing the mandated wholesale regime do not offer any serious threat to the concentrations of private power in the hands of incumbents. At best, mandated wholesale prevents the "outbreak of economic peace" (Davies, 2014, p. 41) that results when the market fully stabilizes around a few large players confined to their respective territorial domains.[203]

While turning away from mandated wholesale would be disastrous for IISPs, extending mandated wholesale to its logical limit would force a radical transformation on incumbents. This would mean abandoning facilities-based competition in favor of service-based competition over

[203] The CRTC acknowledges these domains when it refers to incumbents' "serving territories", in which telcos and cablecos generally "operate exclusively" (CRTC, 2015e, para. 116). The CRTC also distinguishes incumbents operating "out-of-territory" from the rest of a company's operations (CRTC, 2015f).

shared facilities ("structurally separated" wholesale networks), as is the case in a number of national regimes, primarily in Europe (see OECD, 2012). While calls for structural separation[204] in Canada have recurrently been made by some commentators and non-incumbent intermediaries (Rick Adams & Coert, 2014, pp. 7–8; CPAC, 2013a; CRTC, 1994, 2013b, paras. 4373–4385), the dominant view has been that such a policy option is "off the table" (CPAC, 2010) or "not up for discussion" (Palmer, 2015). Structural separation has typically been dismissed as unnecessary and dangerous (CRTC, 1994; Denton, 2013), requiring a more radical disruption of the status quo than Canadian governments have been willing to consider.[205] Near the end of 2016, CRTC Chairman Blais raised structural separation as a possibility for incumbents that "grumble about having to provide wholesale access to their competitors" (Blais, 2016). While these remarks are highly significant, there is no further reason to believe that this regulatory 'nuclear option' (Denton, 2016) is under serious consideration.

If regulatory capitalism designates a mode of governance in which the state focuses on "steering" (directing, guiding) while business concentrates of "rowing" (providing services, entrepreneurship, see Levi-Faur, 2006, p. 505), then Canadian governments have kept the ship on a fixed course for fear of the alternatives. Avoiding the poles of facilities-based and service-based competition means the continuation of liberalization along existing lines, reinforcing the status quo. Mandated wholesale continues precisely because it has not been successful in re-ordering the playing field, and any different course would have consequences that regulators have been unwilling to accept.

[204] See note 137.

[205] At its most extreme, structural separation would have government create a broadband utility providing wholesale access on the same terms to all competitors, thereby neutralizing the advantage that incumbents have by virtue of their control over both long-distance transport facilities and last-mile connections.

Telecom populism

Another factor leading to the federal government's continued support for the mandated wholesale regime is a contemporary form of telecom populism, which has worked against the interests of incumbents (CPAC, 2013b). This has resulted in the coupling of government decisions on intermediary responsibility with the public interest in a way that has not been seen since the battles between Bell and the independents in the early 1900s (see Rens, 2001, pp. 91–97). What distinguishes this from the previous era of telecom populism is the promotion of consumer choice as the objective of competition (CPAC, 2013b).

While policies of marketization (the creation of markets) have a number of other justifications, such as efficiency and international competitiveness, a particularly important reason given in the context of telecom liberalization has been consumer choice. Choice for consumers has been presented as an objective of Canadian telecom regulation since the liberalization of long-distance service (K. G. Wilson, 2000, p. 208; see also Rideout, 2003, p. 166), but was explicitly championed under the Harper government's brand of telecom populism between 2011 and 2015 (Government of Canada, 2013a, 2014). Under this rationale, the greater the number of competitors, the more consumer choice, the better. This makes it hard to accept any policy which would lead to consolidation in the industry, even if such an outcome might reward the success of the most effective competitors.

It was the public's unanticipated interest in the relationship between IISPs and incumbents in the course of 2011 that led to the most recent round of telecom populism, convincing the federal government that there was public interest in the continuation of a mandated wholesale regime that was favorable to IISPs. At the center of the dispute that galvanized public opinion was a CRTC decision about the costs charged by incumbents for wholesale access (CRTC, 2011b). However, this conflict (over usage-based billing, or UBB) quickly became a focal point for concerns over "metered" internet, incumbent dominance of the telecom industry, and the role of the CRTC (Anderson, 2011).[206] In an unprecedented turn of events,[207] a billing dispute between Bell and IISPs became a major political story, and a petition organized by OpenMedia to "demand access to an unmetered Internet" (OpenMedia, 2011) was signed by half a million Canadians. In response, the Prime Minister and Industry Minister both expressed their displeasure with the CRTC's original UBB decision (Chase & Marlow, 2011; Krashinsky, 2011).[208] This led the CRTC to reconsider its decision, thereby demonstrating the limits of the Commission's sovereign authority, which ultimately depends on the support of the federal Cabinet.

For many members of the public who responded to OpenMedia's (2011) *Stop the Meter* campaign, opposing the UBB decision seems to have meant opposing the commodification of bandwidth. For the Commission, the UBB saga demonstrated growing public interest in internet policy and the involvement of new forces (such as OpenMedia and IISP supporters)[209] in hereto

[206] The heart of the regulatory dispute concerned Bell's attempt to charge IISPs for the total amount of data used by their customers (cablecos had already been permitted to engage in this form of billing), and was tied to longstanding concerns among incumbents about "congestion" on their networks (Geist, 2011). This congestion was attributed to "heavy users" (disproportionately IISP subscribers) whose bandwidth consumption had to be "subsidized" by lighter users (House of Commons Standing Committee on Industry, Science and Technology, 2011). Hence, UBB would be a way to compensate incumbents for congestion caused by IISPs and to adjust the behavior of some heavy users by linking usage with willingness to pay. Following Cabinet's intervention, the CRTC reversed its original decision and ruled more favorably for IISPs, but details arising from aspects of the decision would continue to be disputed before the regulator for years to come.

[207] The dimension of public concern over metered access to the internet in Canada echoed American public resistance to telephone companies implementing "measured service" instead of flat-rate billing in late nineteenth-century (see John, 2010; MacDougall, 2013).

[208] Interestingly, both chose to do so through their Twitter accounts, becoming the first time that a change in Canada's telecom regulations was effected by a tweet.

[209] The role of IISPs, and in particular TekSavvy, was highly significant in how UBB initially unfolded as a public issue (M. Geist, personal communication, July 10, 2014). Incumbents have pointed to links between OpenMedia

obscure regulatory disputes.[210] For the Conservative federal government, the issue would become a turning point, leading to more active government involvement in telecom matters and attempts to align policy with public sentiment (M. Geist, personal communication, July 10, 2014).[211] Subsequent to its reconsideration of UBB, the federal government would commit to putting "consumers first" (Government of Canada, 2013a) in the battle for greater telecom competition, with competition defined as greater choice for consumers.[212] The current Liberal government has not been as strident in its pursuit of telecom competition, but its official statements continue to emphasize the importance of consumer choice (Government of Canada, 2016).

Shifting the goalposts: The middle mile as the middle road

Finally, it is important to note that even as the CRTC claims to adhere to the rationality of facilities-based competition, it has become increasingly convinced of the inadequacy of this approach, applying further regulation to facilities-based incumbents and according more

and IISPs such as TekSavvy and, such as the funding that OpenMedia receives from IISPs and how the organization promotes IISPs and their interests (CRTC, 2011e; TELUS, 2015). For its part, OpenMedia lists IISPs among its "network" of supporters, who provide "donations, expert input, and collaborative support on various campaigns", but claims this network has "no direct operational input" into OpenMedia's activities (OpenMedia, 2015, p. 3).

[210] The first internet policy debate in Canada that generated widespread public interest occurred over copyright reform during 2007-2008 (what Haggart [2014] calls the "Canadian Facebook Uprising"), and did not involve the CRTC. The Commission has seen broader public broader public participation through a growing number of submissions filed by individuals in recent years, on issues that previously would not have been raised, or which would only have received input from intermediaries (see Ryan Adams, 2015; Klass, 2013; Roseman, 2012). Notably, the UBB saga included involvement by Jean-François Mezei (Chase & Marlow, 2011), who has subsequently filed submissions and appeared before the Commission on various proceedings.

[211] A former CRTC Commissioner described it as "the first time a government realized it could lose an election on an apparently obscure issue of telecommunications policy" (T. Denton, personal communication, November 12, 2014).

[212] The government's commitment to this objective led to an unprecedented conflict with the "big three" wireless incumbents (Bell, Rogers, TELUS). In the public-relations firestorm described as the "telecom war" of 2013, both sides invested heavily in ads designed to generate public support for their respective visions of competition (Dobby, 2014a). For incumbents this meant a "level playing field" (Bell et al., 2013a; Bell, Rogers, & TELUS, 2013b), while government tried to encourage a new competitor (for a time, widely understood to be US-based Verizon) to compete against the three in an upcoming spectrum auction.

legitimacy to leased (wholesale) access (Denton, 2013). In its recent FTTP wholesale decision (CRTC, 2015e), the regulator has apparently changed the meaning of facilities-based competition, with a new focus on middle-mile networks (Karadeglija & Shekar, 2015). This reorientation may yet transform failure into success by shifting the regulatory objective, and justifying the indefinite extension of mandated wholesale.

At the wholesale access review that brought about this regulatory shift, IISPs made the argument that facilities-based competition need not refer to competition between complete sets of facilities, because some kinds of facilities (particularly those for last-mile access) cannot or should not be duplicated. According to this view, the ladder-of-investment does not need to lead "to some oddly-configured world of a third, fourth, or fifth wireline access to every home or business. [Instead], different ladders lead to different places" (CNOC, 2014, p. 4). Rather than extending as many complete last-mile networks as possible, with each running its own wires to potential customers, competition between facilities might take place at the "middle mile", where infrastructure investments make more sense for smaller players (Henderson, 2014c). During the same review, Rogers also argued that there is little reason to expect anyone to build a third wired network where two are already in place (the local telco and cableco), and that the wholesale access regime should be treated as permanent rather than temporary (CRTC, 2014g, paras. 8720–8721).

As a result of the wholesale access review described above, the CRTC extended mandated wholesale access to FTTP and claimed to continue its support for facilities-based competition (CRTC, 2015e). The decision stated that the dominance of facilities-based carriers is built on the advantages created through decades of incumbency, and that considerable barriers to the deployment of these facilities exist for non-incumbents. The CRTC has therefore concluded that it is neither "practical or feasible for competitors to duplicate" the last-mile fibre networks being deployed by incumbents (CRTC, 2015e, secs. 134–136), and mandated wholesale access to these facilities. At the same time, the CRTC changed wholesale obligations for "middle-mile" portions of broadband networks as a way to encourage IISPs to invest in these facilities (Karadeglija & Shekar, 2015).[213] The decision leaves the scope of facilities-based competition up for debate, suggesting that only some kinds of facilities will compete in the future, while others will be leased. Mandated wholesale access to the last mile is clearly part of the current approach, but competition in the middle has become the middle road between structural separation and deregulation.

The limits of competition

This chapter has traced the development of regulation-for-competition in Canadian telecom and the mandated access regime. Consistent with the larger phenomenon of regulatory capitalism, Canadian telecom is governed through norms and regulations that specify how intermediaries should compete with one another, and where they should avoid competing. This regime has failed in its original objective to foster an arrangement of intermediaries that engage in facilities-based competition, as evidenced by the continuation and expansion of mandated access. The reasons for the regime's failure can be linked to flawed assumptions about how incumbents and new entrants would behave following liberalization, but I have been more

[213] This was achieved by imposing "disaggregated service" for those wishing wholesale access to FTTP networks, meaning that (in)dependent ISPs would be responsible for getting their traffic to and from access points near the last mile, through the use of their own (owned or leased) middle-mile networks. The CRTC (2015e), also eliminated mandated wholesale access to "unbundled local loops", used to provide low-speed internet access over legacy telco infrastructure, effectively upgrading wholesale obligations to the era of fibre networks.

interested in accounting for the regime's continuation than its failure. The reasons why mandated access continues to endure as a central point of struggle over telecom policy includes the CRTC and federal government's unwillingness to accept either of the two main alternatives to the regime: allowing complete incumbent dominance (by eliminating mandated access) or removing incumbent control over both facilities and services (through structural separation). Dismantling the mandated access regime would contradict the government's longstanding emphasis on maximizing consumer choice – a cause that was taken up fervently in the later years of the Harper Conservative government as a kind of telecom populism that opposed incumbent interests. Finally, it is worth remembering that while promoting competition remains the governing rationality for telecom regulation, what this means has changed over the years.

Facilities-based competition is still “typically regarded as the ideal and most sustainable form of competition”, but it “is best achieved by requiring incumbent carriers to make available facilities that are 'essential' for competition” (CRTC, 2015e, secs. 5–6). This means that incumbents' ownership of their most strategic resources – 'bottleneck' facilities – also obliges them to share these facilities, rather than treating them as a source of competitive advantage. If the CRTC decides that facilities-based competition does not require competing wires at the last mile, then it can be achieved by competing backbones at the middle mile. Rather than some imminent end-state where regulators can depart from the stage, the current form of facilities-based competition points to a world where some classes of facilities are shared while others compete, and regulators guard the distinction between the two. Mandated access responsibilities and the power imbalance between IISPs and incumbents will continue to be part of this picture, while new struggles are fought to delineate the boundaries of acceptable competition.

The rationality of facilities-based competition may shift to achieving a different outcome than initially imagined, or competition between a particular subset of facilities, but the value of competition in Canadian telecom remains dominant. Network-building can be justified for reasons other than enabling private sector competition, but the competitive ideal is never disputed. The problem is never too much competition, or too great a reliance on markets. If there is a problem, it is either that there is not enough competition or that it is the wrong kind (facilities or service-based). Since intervention in the market is justified as regulation-for-competition, and because the ultimate vision of a competitive market desired by these public policies is never clearly laid out, the resulting arguments can be dizzying in their contradictions. Where potential competitors are forced to cooperate by sharing infrastructure, this is justified as a way to promote competition. Competition requires a level playing field, which is promoted through differential treatment – imposing responsibilities on the most powerful and sustaining intermediaries that would otherwise be unable to sustain themselves.

Ultimately the debates in this chapter have been less about competition and more about power. This is often openly acknowledged, since notions of competition and market power are deeply interrelated in regulatory policy. The CRTC decisions underpinning the mandated wholesale regime are more appropriately thought of as a way of restraining industry power, rather than a means of promoting industry competition. Under the logic of liberalization, one is presumed to lead to the other, but this is not necessarily the case. Incumbent power is controlled through the mandated access regime, just as it is through spectrum auctions and merger approvals, but the result has not been a flowering of competition. Instead, liberalization has led to a concentration of power in the giant firm(s), and regulations have placed boundaries around this consolidation.

By keeping its policy orientation vague, the CRTC furthers its exercise of power on these issues. By avoiding interpretive constraints (such as what facilities-based competition actually aims towards), the regulator can maintain flexibility in how it rationalizes individual decisions. Even without an alternative vision of how to organize telecom infrastructure in Canada, preventing the giant firm's ultimate triumph (symbolized by the recurrently-raised possibility of a Bell-TELUS merger, see Marowits, 2007; Nowak, 2009) remains an important public policy objective. But limiting corporate concentration is a shallow political vision compared to pre-1990s notions of national digital infrastructure (see Mussio, 2001), or the principled pursuit of competition that was espoused at the outset of liberalization. And so, public policy that was once meant to shape a new arrangement of market actors is left maintaining the existing order – and order which preserves incumbent dominance as well as the opposing tension brought by IISPs.

These opening chapters have addressed the political economy and structural arrangement of the telecom industry in Canada, as the product of the monopoly era, liberalization, the emergence of internet intermediaries, and regulatory capitalism. The next two chapters deal with some of the responsibilities that intermediaries must contend with in this environment, as they pertain to digital flows and information – namely privacy, copyright, security, and net neutrality.

Chapter 4: Privacy custodians

In keeping with the protocol or etiquette developed in the usage of the internet, some degree of privacy or confidentiality with respect to the identity of the internet protocol address of the originator of a message has significant safety value and is in keeping with what should be perceived as being good public policy.
-Justice von Finckenstein (*BMG Canada Inc. v. John Doe*, 2004, para. 37)

This chapter is about how intermediaries govern the privacy of their subscribers and users, and how this role has developed over time. On a recurring basis, expectations that intermediaries should act as guardians and caretakers of personal information have competed or conflicted with other pressures and public policies, including copyright, policing and cyber security. The fundamental role of privacy considerations within these other public policy areas means that it is impossible to understand intermediaries as instruments of surveillance, identification, policing, and security without also appreciating their roles as privacy custodians. Where ISPs have access to vast amounts of sensitive personal information about their users – including their browsing histories, interests, habits, and secrets – they act as privacy custodians by "guarding the link between the information and the identity of the person to whom it relates" (*R v. Spencer*, 2014, para. 46). Where ISPs are conduits of information, they act as privacy custodians by guarding the privacy of these communications. Intermediaries also act as privacy custodians by limiting the amount of information they collect, even though such collection might be easy and beneficial for other reasons.[214] Privacy custodianship is not just limited to the

[214] For instance, some Canadian ISPs utilize deep-packet-inspection (DPI) technology in order to differentiate between kinds of traffic (Bendrath & Mueller, 2011; Parsons, 2013). This is a kind of surveillance for routine traffic management and network operations, and must be limited to these uses to remain consistent with intermediaries' obligations as privacy custodians (see TekSavvy, 2016). These obligations require intermediaries to obtain consent before any collection of personal information, to specify the purpose of this collection and to limit collection to what is "necessary" for its specified purpose (see Lawson & O'Donoghue, 2009, p. 35). In other words, while DPI technology can be used in an invasive manner to build valuable records of users' online

obligations specified by privacy law, but refers more broadly to how personal information is governed by these institutions.

Finally, the role of a privacy custodian extends beyond its relationship with users and their personal information, but is played out through a broader relationship with the public. This includes efforts by some intermediaries to educate the public about privacy, as well as the accountability regimes through which intermediaries report how they gather, handle, and disclose personal information.

However, because of the limited scope of such accountability, the extent to which ordinary users and customers must depend on their privacy custodians, and the flexibility that intermediaries have in meeting their legal obligations, privacy stewardship is a relationship based largely on trust (see Kerr & Cameron, 2006, pp. 272–273). We can trust or distrust our intermediaries to protect our information and our identities. Intermediaries seek to reassure us and to demonstrate their trustworthiness. Incidents such as the Snowden disclosures can therefore have a significant effect on this relationship (see Sargsyan, 2016; TekSavvy, 2014, p. 2) without altering intermediaries' legal obligations.

The questions that this chapter asks are: How do intermediaries in Canada manage their role as privacy custodians and these attendant responsibilities, alongside their sometimes conflicting roles assisting government agencies and other organizations investigating their customers and users?[215] In other words, this chapter analyzes the "role conflicts"[216] that

activities (Gallagher, 2012), intermediaries using this technology are expected to remain largely oblivious to what their users are doing.

[215] For example, in the circumstances of the investigation that led to early cybercrime case of *R. v. Weir*, the ISP was forced "to intermediate between two potentially conflicting roles: (1) its role as the trusted steward of its clients ' personal information and private communications; (2) its role as a party in possession of information that might assist in law enforcement" (Kerr & Gilbert, 2004, p. 165).

[216] See note 26 above.

intermediaries must navigate as they act as privacy custodians, governing both personal information and the privacy of communications. Intermediaries maintain repositories of personal information about their users, including their names and addresses, and IP logs. As the internet's gatekeepers, intermediaries are also in a position to surveil traffic passing through their networks. Other institutions carrying out internet surveillance (advertising networks, online platforms, intelligence agencies) monitor users as they interact with portions of the internet, or as their traffic passes through particular nodes. But ISPs sit directly upstream and downstream from their subscribers, which in theory gives them access to the “full pipe” of their subscribers' traffic (Fung, 2016),[217] and ISPs are required to routinely monitor activity on their networks.[218] The question of what kinds of traffic should be monitored, what information should be retained about subscribers, and whether ISPs should share this information with other actors, necessarily implicates these institutions' roles as privacy custodians.

In broad terms, privacy custodians are subject to both positive and negative legal obligations, and these legal requirements shape the practical rationality that intermediaries employ to protect privacy. Canadian ISPs are subject to the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*),[219] which imposes positive responsibilities around

[217] This assumes the data is not encrypted or otherwise protected.

[218] At a meeting of the IETF in the immediate wake of the Snowden disclosures (IETF 88 in November 2013), during a discussion of how to better protect internet traffic from “pervasive surveillance”, one participant (Bill Mitchell) raised the following concern (which the meeting's chair, Stephen Farrell, characterized as “a tension”): "I'm kind of concerned when I think about an ISP or someone who is actually doing network operations... that one of their primary jobs is monitoring, and traffic engineering, and billing. So they need to track, they need to monitor, they need to surveil. Are we trying to prevent operations people from doing their jobs?” (*IETF 88 perpass “BoF” session*, 2013).

[219] *PIPEDA* is the federal private-sector privacy law (whereas federal government departments are subject to the *Privacy Act*), which has governed the responsibilities of internet and telecom service providers as privacy custodians since the act gradually went into effect in the years following 2001. Many obligations under *PIPEDA* echo those found in other Canadian privacy laws. Commonalities can be traced to voluntary guidelines adopted by the OECD (1980), to which Canada expressed its commitment in 1984 (Bernal-Castillero, 2013), and which also form the basis of privacy laws in numerous other countries. While *PIPEDA* imposes the most relevant

accountability,[220] identifying the purposes of collection and obtaining consent, ensuring accuracy of information, and using appropriate safeguards (Government of Canada, 2000, schedule 1). However, the privacy responsibilities that have been at the center of internet policy debates are expressed primarily in negative terms. These are obligations *not* to collect, use, or disclose personal information, or to place specific limits on these activities (Government of Canada, 2000, schedule 1, clauses 4.4-4.5). These negative responsibilities may conflict with positive pressures that encourage or require intermediaries to do the opposite.

It is important to note that the above distinction between negative and positive duties or responsibilities is not always straight-forward. Many negative responsibilities have a corresponding and equivalent positive responsibility, and vice versa (M. G. Singer, 1965). For example, the positive duty to obtain consent before disclosure can be considered a prohibition against disclosure without consent. An obligation to openness, accuracy and accountability has a corresponding obligation not to be secretive and misleading. But many responsibilities listed above do not necessarily have this kind of positive/negative equivalence.[221] One of the most important responsibilities for this analysis is the limitation on disclosure, which is essentially negative, and requires some additional reasoning to translate to a positive duty. However, this is precisely what some intermediaries have done in several cases (Distributel, 2013; *R. v. TELUS*, 2013; *R. v. Rogers*, 2016; *BMG Canada Inc. v. John Doe*, 2004), by interpreting the limitation of

responsibilities for intermediaries as privacy custodians, it should be noted that the CRTC and some of its regulations also confer privacy protections for subscribers (CRTC, 2003a, 2003b, 2009c; Karadeglija, 2014a; Public Safety Canada, 2012d, p. 258). Interestingly, one set of regulations isolates customer information held by an incumbent's wholesale operations from its retail operations (CRTC, 2011d), creating an internal barrier to information sharing within incumbent ISPs that is intended to protect competition (see note 194).

[220] This includes designating an individual responsible for privacy, often known as a Privacy Officer. Other sections of *PIPEDA*'s Section 1 oblige institutions to be accountable to individuals who want access to information about themselves, or who want to know how this information has been used and disclosed.

[221] For instance, it makes little sense to think of an obligation to limit collection as having a corresponding positive responsibility, unless we think of enacting limits as an action in the positive sense.

disclosure as obliging them to take certain actions in order to protect their users. Hence, my argument is that in recent years, some intermediaries have been adopting more of a positive orientation towards their responsibilities as privacy custodians. This also means they have demonstrated a greater degree of agency in determining what it means to play the role of privacy custodian. Rather than a legal standard which institutions must meet, some organizations have treated privacy as a value to fight for, even if this means challenging state actors or opposing court orders. This trend reflects a growing recognition of the important role played by privacy custodians, and the efforts of some organizations to differentiate themselves by demonstrating (rather than merely stating) their commitments to the privacy of their users. However, this trend has been neither consistent nor strong, since intermediaries' roles as privacy custodians are continually in conflict with contradictory pressures.

I have previously argued that intermediaries, whether these are massive corporate ISPs or FreeNets, can be understood as collective actors, in that they exercise a degree of autonomy when making decisions such as whether or not to cooperate with law enforcement, or what it means to safeguard their users' privacy. We can see this through the different approaches that ISPs acting as privacy custodians have taken on issues such as privacy policies (Clement & Obar, 2015), the amount of time these companies choose to retain personal information (Gaudrault, 2012a; sssscary, 2012), how ISPs respond to copyright notices (Geist, 2015; Government of Canada, 2009), and in how they share information for reasons of security and law enforcement (Parsons, 2015b). For each of these questions, intermediaries must find ways of resolving the tensions around their responsibilities as privacy custodians when these conflict with other roles, and are subject to contradictory pressures. These pressures can be applied by copyright owners (Eby, 2008), government agencies (CBC News, 2009), or result from an intermediary's own desire to collect and use personal information in the pursuit of greater profits (Office of the Privacy Commissioner, 2015b). In opposition to such forces, intermediaries have also been called upon by their customers and other critical public voices to strengthen privacy protection or be more accountable in their role as privacy custodians (Clement & Obar, 2015; Freeze, 2014; Gaudrault, 2012a; Henderson, 2014b; sssscary, 2012).

As privacy custodians, intermediaries must safeguard communications and personal information, and be accountable to their users regarding these practices. In their surveillance roles, intermediaries collect and disclose information, and are often prohibited from notifying their users or the public of such activities. Alternately, intermediaries might have other reasons to surveil their users (for profit, or network management), and find ways of reconciling these actions with privacy commitments. While those advocating for surveillance practices often claim that intermediaries can collect or disclose personal information while respecting privacy, the contradiction between the two has been made clear through a number of legal contests covered in this chapter.

For ISPs acting as privacy custodians, accommodating some desires or expectations inevitably creates tension with others. Satisfying the privacy or surveillance demands of certain groups results in dissatisfaction for those pulling in the opposite direction. In response to such dissatisfaction, privacy custodians have frequently justified their actions as being limited to, or constrained by, what is required of them by law (Gaudrault, 2012b; Karadeglija, 2014b; Ling, 2014; Mediacaster, 2011). And yet, companies operating in the same legal jurisdiction have taken rather different approaches in interpreting just what their legal obligations consist of.

Indeed, citing what is “required by law” can obscure the amount of latitude that intermediaries have in their actions, including the choice to test or challenge the law (see *R. v. TELUS*, 2013; *R. v. Rogers*, 2016). Intermediaries thereby minimize their agency, even as they exercise it.[222] Intermediaries have also collaborated with each other to establish common policies, practices, and approaches to privacy-related issues (see Government of Canada, 2009; Morin, 2011), but the conduct of privacy custodians across the industry has been far from uniform.

The variability in how intermediaries govern privacy is partly related to their diversity as actors in the context of regulatory capitalism, as compared to the uniformity of the monopoly era. Private ISPs compete while meeting public policy objectives, and may even compete on the basis of how well they meet these objectives, treating privacy as a product differentiator. As discussed in the following chapter, this diversity of actors and approaches has been a problem for police and security agencies, since some intermediaries have been more willing than others to utilize *PIPEDA*'s “lawful access” exceptions. However, the roles of intermediaries as privacy custodians developed before *PIPEDA* and the internet, and it is to this history to which I now turn.

Pre-internet intermediaries as privacy custodians

While the expectations applied to intermediaries in Canada varied over the course of the nineteenth and twentieth centuries, the idea that these organizations had a duty to protect the privacy of the communications is almost as old as the idea that they had a duty to help law

[222] Intermediaries typically provide little detail about how they exercise discretion when receiving government demands for information (Parsons, 2017), and sometimes provide misleading accounts using terms such as “voluntarily”, “turn over”, or “required”. For instance, a blog post titled *Proud of our commitment to privacy in Canada*, stated that “TELUS regularly assists law enforcement agencies in obtaining customer information they need for an investigation – but only when TELUS is ordered by a court to do so... we never voluntarily turn over customer information” (Blackburn, 2013). During this time (prior to the 2014 *Spencer* decision), voluntary disclosures of customer information by TELUS, as justified by *PIPEDA* section 7(3)(c.1), are well-documented (Ling, 2015) and admitted by the company elsewhere (TELUS, 2014).

enforcement. Initially however, the greatest threats to the privacy of users came from telephone company employees as well as other subscribers. The early telephone system depended on human operators (typically women), who were required to listen to calls to do their job.[223] In 1899, Bell enacted regulations to protect the confidentiality of conversations, requiring operators to listen only to the "sound" of conversation and ignore the meaning (Martin, 1991, p. 69). "Listening on the line" was a violation of company rules and regulations, and was eventually made illegal, but the practice was apparently widespread in Canada during the early twentieth century (Martin, 1991, pp. 107–108). Legislation was passed to ban operators listening to calls in Quebec in 1918 after an MLA recounted an event in which a Bell company official, joined by an operator, interrupted a conversation between a man and woman to give the man "a severe talking to" ("Eavesdropping on 'phones an offence," 1918; Martin, 1991, p. 107; National Assembly of Québec, 1918).

Privacy was less of an expectation in rural Canada, and norms of behavior were different. In order to save costs, rural telephone service was most often carried out over a "party line" (Rens, 2001, p. 87) that served up to thirty subscribers.[224] Only one call could be carried by the line at a time, but multiple subscribers could listen in. Indeed, it was often expected that one's

[223] Martin (1991) refers to operators as "human mediators" (p. 50) who needed to be subordinated to the company's rules and policies. In 1907, operators in Toronto went on strike and the public learned about the women's poor treatment and work conditions. In the course of a Royal Commission, concern over the health of the "weaker sex" quickly shifted to the possibility that calls were being intercepted inappropriately (Sangster, 1978, p. 119) – an early example of Canadian concerns over the conduct of privacy custodians.

[224] Michéle Martin (1991), drawing on the archives of Bell Canada, notes a "tension between the obligation to provide privacy for the customers who paid the most and the obligation to extend service to the other classes as a public utility was present throughout the period studied [1876 to 1920]" (p. 49). The party line was more common in the telephone's early development, which she likens to a "public place in which people sought to have private conversation" (p. 52). Poor wiring in early telephone systems also led to cross-talk, with conversations leaking between lines (p. 143). Private lines were promoted as the answer to privacy concerns, and automatic switchboards later replaced the need for operators (pp. 144-145; see also Babe, 1990, p. 278, note 60), but these advances first became available to wealthier urban users, and party lines persisted in rural Canada through the 1990s, serving around 145,000 subscribers in 1997 (Rens, 2001, p. 339).

neighbors would be listening on the line, and a conversation between two parties could turn into a group discussion.[225] One doctor who operated a telephone network frequently listened in to calls, and had a "penchant for argument" – interrupting conversations to give his opinion (Babe, 1990, p. 83).

Companies were subject to provincial legislation in Ontario and Quebec that regulated eavesdropping and made it an offence to divulge the content of a telephone conversation (Cornfield, 1967, p. 112; Martin, 1991, p. 145). Manitoba and Alberta both explicitly prohibited wiretapping (Canadian Committee on Corrections, 1969, p. 82; Cornfield, 1967, p. 112; Rahamim, 2004, p. 90).), but this did not apply to Edmonton's municipal telephone system. From this legal "patchwork" (Molinaro, 2017, p. 464) , general privacy laws developed gradually in Canada over the latter half of the twentieth century and into the twenty-first (S. A. Cohen, 1982, pp. 665–667; Cornfield, 1967; Power, 2013). However, the eavesdropping and surveillance restrictions that did exist often did not apply to police investigations, so formal requirements for intermediaries to assist police in intercepting communications were rarely stated explicitly (Cornfield, 1967, p. 112).[226] Intermediaries (specifically, telephone and telegraph companies) did apparently assist police investigations and enable wiretaps, either voluntarily or based on the understanding that they were required to do so, but the extent and nature of this surveillance is unclear.[227] In large part, this was due to the fact that there existed no federal

[225] Eavesdropping was also not seen as negatively among rural telephone users, and may have been interpreted more as participation in community life or simply keeping up with the local news (Martin, 1991, pp. 152–153).

[226] The situation was complicated by jurisdictional issues and the lack of a nation-wide telephone monopoly. While Bell dominated Ontario and Quebec and was subject to the Bell Canada Act, other telephone companies operated under provincial or municipal jurisdiction (Chorney, 1964, pp. 441–445)
(Chorney, 1964, pp. 441–445). In Edmonton for instance, the Chief of Police requested and received an amendment to the bylaw governing the municipal telephone system in 1965, permitting a magistrate to authorize a wiretap (Cornfield, 1967, p. 112).

[227] In 1969 the Chief of the Toronto Police stated that while his department had been tapping phones since 1966,

prohibition against wiretaps (Canadian Committee on Corrections, 1969, p. 82), and police officers in much of Canada arguably had the authority to direct intermediaries to disclose private communications (Chorney, 1964, pp. 449–450). For much of the twentieth century there also existed no right to privacy in Canada, and wiretapping was not a common law or criminal offence, making it difficult to challenge a police wiretap (Rabideau, 1991, p. 172). The rules that did exist prohibiting intermediaries divulging private communications could be overcome through some form of “lawful authority”. While what this entailed (whether a court order or a simple police request) was unclear, police appear to have successfully asserted their authority to make such demands or requests.[228]

In 1969 the *Quimet Report* (Canadian Committee on Corrections, 1969) recommended greater control over electronic surveillance and accountability for its use, leading first to police guidelines, and then the *Protection of Privacy Act* in 1974 (Hubbard, Brauti, & Fenton, 2015, sec. 1.1.1; Rabideau, 1991, pp. 172–173). The *Privacy Act* amended the *Criminal Code* to criminalize the “invasion of privacy” as well as formalizing the exemptions to such an offence.

they had “no formal, or informal, liaison with the telephone company on wiretapping, but he added: 'The company does assist in other ways.' He did not say what 'other ways' were involved” (Burns, 1969, p. 2). Information obtained through wiretaps was generally not used as evidence in court (see “RCMP bypassed Bell, pried open terminal box to tap apartment phone,” 1977; Winsor, 1973), partly because of fears that its legality would be questioned (such as in relation to the Bell Telephone Company of Canada Act’s prohibition on interference and interception, see Burns, 1969; Claridge, 1972). The RCMP did maintain an extensive but highly secret wiretapping program in cooperation with Bell and the British Columbia Telephone Company for national security purposes from 1951 into the 1970s (Molinaro, 2017). However, it seems that prior to 1974, wiretaps were frequently installed without the explicit knowledge of the telco, particularly in apartment buildings where police would simply break into Bell's equipment (“RCMP bypassed Bell, pried open terminal box to tap apartment phone,” 1977).

[228] Interestingly, in 1947 Bell was approached by the Ontario Provincial Police, who wanted to serve the company with a search warrant to trace calls. Bell was opposed, and agreed to send the matter to court (to quash the warrant) as a test case. The High Court of Ontario ruled in Bell's favor and against the warrant (Cornfield, 1967, p. 113). The following year, Toronto police sought a *Criminal Code* amendment to permit a judge to authorize them “to enter a telephone exchange and by the attachment of certain apparatus secure information being communicated by suspected persons.” Bell successfully opposed this recommendation in part as “an infringement of private rights”, and also out of a fear that the power could be “extended indefinitely” (Conference of Commissioners on Uniformity of Legislation, 1948, pp. 36–37). Subsequently, police came to maintain that they themselves had the lawful authority to authorize a wiretap (Cornfield, 1967, pp. 113–114).

These exemptions specified when forms of electronic surveillance were not considered a crime, such as when carried out under judicial authorization (Hubbard et al., 2015; Rahamim, 2004, pp. 90–94). The 1974 amendments thereby formalized the authority under which police (or intermediaries working on their behalf) could carry out surveillance, and established a hierarchical relationship between the roles and responsibilities of intermediaries. "Invading" the privacy of subscribers was now a criminal act, thereby constraining intermediaries as carriers of communications, and obliging them to respect the privacy of subscribers. However, the exemptions listed in what would become Part VI of the *Criminal Code* effectively trumped this negative responsibility, specifying instances in which privacy invasions could be justified or legally authorized. Intermediaries now clearly had a vital role to play in safeguarding privacy, but their privacy obligations were secondary to their judicially-authorized surveillance responsibilities. Additionally, the prohibitions against privacy invasion could be voluntarily overcome by intermediaries for other reasons, such as when necessary to provide a service or in the interests of safeguarding subscribers.[229] By the 1990s, the legal authorities under which police could demand or request access to subscriber communications or records held by telcos were fairly clear, but the attempt to extend such rules to cover ISPs would set off lengthy and contentious debates.

[229] These are Sections 184(2)(c) and (e) of the *Criminal Code*, which exempt telecom personnel from the s. 184(1) offence of unlawful interception in the performance of certain duties. The Ontario Court of Appeal case *R. v. Fegan* in 1993 tested the limits of this exemption. Bell personnel had carried out an investigation into harassing telephone calls against women using the Bell network. The court ruled that Bell could legally use a digital number recorder (DNR) in the pursuit of its investigation (Hubbard, Brauti, & Fenton, 2015, sec. 2.3).

Invisible handshakes and internet surveillance

The early public internet of the 1990s was far from an ungoverned, lawless domain, but police forces in general devoted little attention to combating 'cybercrime', and saw little value in online investigative and surveillance techniques until the end of the decade. It was common to associate the rise of internet connectivity and borderless online services with arguments for the “decline of the state” in a globalized, privatized world (Birnhack & Elkin-Koren, 2003, p. 2; Goldsmith & Wu, 2006). However, state agencies soon came to appreciate the role that the internet played in society, and what opportunities it afforded for social control. According to Birnhack and Elkin-Koren (2003), ordering the online field was initially left to the “invisible hand” of the market and the new private intermediaries. However, in the 2000s, state agencies returned to make an “invisible handshake” with these intermediaries, recruiting and co-opting them towards state goals. Data packets may frequently cross international borders without inspection, but they are carried over a physical transport infrastructure that is by necessity, a local asset, and therefore subject to state control (Goldsmith & Wu, 2006, p. 73).[230] Governments recognized that the cooperation of ISPs would be key to policing and surveillance in the online era, and some of these ISPs (the telco incumbents that emerged as ISPs in the mid 1990s) were already familiar partners for state agencies.

Birnhack and Elkin-Koren worried that the incentives for ISPs to cooperate with state agencies would create an “unholy alliance” between the two (2003, p. 4). A similar concern developed regarding the pressures that intermediaries were under from copyright owners, who sought to control infringement on their networks and services. Industries that were heavily-

[230] This is also why Sargsyan (2016, p. 2223) argues that requirements to locate data within certain jurisdictions, supposedly to protect privacy, can “increase the effectiveness of law enforcement, grant governments more jurisdictional control over data, and amplify governments’ surveillance potential”.

invested in copyright had significant influence over government policy in a number of countries (principally the US),[231] and it was feared new laws might compel ISPs to act as copyright police. Some also argued that intermediaries and copyright owners would find common cause to cooperate, in that file-sharing traffic was a major cause of network congestion, and that vertical integration meant intermediaries might have a stake in controlling the availability of content (de Beer & Clemmer, 2009, pp. 405–406). What these authors did not fully appreciate were the ways that the interests of intermediaries, state agencies, and copyright owners were fundamentally misaligned. Such conflicts came dramatically to the fore in battles over copyright reform, where the business models of intermediaries and copyright owners were at odds (see Edwards, 2011; Horten, 2012).[232] When it came to state surveillance efforts, ISPs were more willing to act as deputies or partners, but even this cooperation had its limits, and the tension became more pronounced following the Snowden disclosures of 2013. In both cases – copyright enforcement and state surveillance – ISPs' roles as privacy custodians would come into conflict with expectations that these institutions would act as internet police or surveillance deputies. However, it was in a legal dispute concerning copyright that Canadian ISPs would first assert the privacy interests of their subscribers, interpreting a negative responsibility not to disclose information as a positive duty to oppose such disclosure.

[231] The position of the US government on intellectual property has been particularly consequential for the rest of the world, because of the way that the intellectual property interests of American industries have been promoted as a condition of signing trade treaties with the U.S. (Braithwaite & Drahos, 2000; Drahos & Braithwaite, 2003; May, 2010; May & Sell, 2006).

[232] In Canada, these battles played out in respect to proposed amendments to the copyright act since the early 2000s, which were finally enacted through Bill C-11 in 2012 (Doyle, 2006; Government of Canada, 2012; Haggart, 2014).

Privacy & piracy

In 2004 a group of incumbent ISPs[233] took an active stand to protect the privacy of their subscribers against a group of copyright owners.[234] In what would become a landmark legal decision (*BMG Canada Inc. v. John Doe*, 2004), the ISPs acted to safeguard the interests of their customers: the “John” and “Jane Does” whom copyright owners sought to identify. The copyright owners presented a list of IP addresses collected by the copyright surveillance company MediaSentry, which had identified these addresses as sharing copyrighted music. In order to link these same IP addresses to internet subscribers who could be sued for copyright infringement, the copyright owners needed the help of ISPs. However, privacy law seemed to demand that ISPs should protect this information. The Federal Court was in a position to decide between these competing demands, and had the power to order[235] the ISPs to cooperate.

The relevant aspects of the case described above (known as *BMG Canada Inc. v Doe*), besides its long-lasting consequences for Canadian law (Knopf, 2013), were the different positions taken by the five ISPs involved. All were acting as privacy custodians for their respective “Does”. The companies were "trusted holders” of these subscribers' identities (Kerr & Cameron, 2006, p. 272), but how they acted on this responsibility varied. Importantly, some ISPs rationalized their role as privacy custodians in a way that included a positive responsibility to assert the privacy rights of their subscribers. Others adopted a more negative orientation – treating privacy responsibilities as a set of conditional obligations *not* to disclose personal

[233] Specifically, Bell, Rogers, Shaw and TELUS, alongside the Electronic Frontier Canada (EFC) and the Canadian Internet Policy and Public Interest Clinic (CIPPIC), who acted as interveners in the case.

[234] The copyright owners consisted of seventeen music recording companies who were members of the Canadian Recording Industry Association (CRIA).

[235] The kind of court order used to compel information held by a third party in order to facilitate a lawsuit is known as a *Norwich* order, following English jurisprudence (Smith, 2007, pp. 441–447; Vermette & Iatrou, 2010).

information. The case would be an important early episode in a process which would see some intermediaries adopt a more positive conception of privacy stewardship.

The lowest degree of involvement in *BMG Canada Inc. v Doe* came from Vidéotron, which chose not to participate in the court proceedings. The company's guardianship of its subscribers' identities amounted to waiting for the court order to be issued before these identities were disclosed – a position that could be attributed to the company's various media interests and its general opposition to "piracy" (Kerr & Cameron, 2006, p. 290; Pacienza, 2004; Thompson, 2004; see also Wire Report, 2008).[236] This was a negative rationalization of the company's privacy responsibilities, which were interpreted as a prohibition against disclosing customer information to a private party in the absence of a court order.

On the other hand, Shaw provided the greatest resistance to the motion, pushing back to protect the privacy of the company's customers (Kerr & Cameron, 2006, p. 278; Pacienza, 2004; Shaw, 2004; G. Shaw, 2004; Thompson, 2004).[237] The positive duty of a privacy custodian expressed by Shaw amounted to asserting the privacy rights of the company's anonymous subscribers, by making arguments on their behalf to oppose the court order sought by the copyright owner. Meanwhile, Bell (2004) and Rogers (2004) both submitted privacy-related arguments,[238] and TELUS (2004, p. 2) complained about being conscripted to carry out

[236] Vidéotron is owned by Quebecor Media. After the motion to identify the subscribers was denied by the Federal Court, the copyright owners appealed the decision. Rather than oppose the appeal, Vidéotron supported the appellants and stated that while the company "agrees to protect its clients' privacy... [it] does not agree to protect its clients' piracy" (Vidéotron, 2004, p. 13).

[237] In its written submission to the Court, Shaw cites its privacy policy: "Customer privacy is a high priority at Shaw as we have always maintained a policy of protecting our customers' personal information." It is this publicly stated commitment to protecting the privacy of Shaw's customers' personal information that in large measure dictates Shaw's response to this motion. Shaw believes in this policy" (Shaw, 2004, p. 6).

[238] However, Bell's (2004) argument largely consisted of laying out its obligations under *PIPEDA*, while Rogers argued that some of the information sought by copyright owners was "overbroad" and "excessive" (Rogers, 2004, p. 6).

investigations for the copyright owners, which might result in the company being sued by its own customers (Kerr & Cameron, 2006, pp. 278–279).

In *BMG Canada Inc. v Doe*, numerous other elements were in dispute besides how Canada's new privacy legislation[239] should apply to ISPs. The intermediaries made arguments about copyright law, the costs of identifying their customers, MediaSentry's evidence, and whether the sort of identification sought by copyright owners was even possible to carry out accurately. In the end, Justice von Finckenstein[240] denied the copyright owners their motion on several grounds and refused to grant a court order to compel the ISPs to identify their customers. Some of his reasons were upheld when an appeals court subsequently dismissed the case, and while that decision left the door open for copyright owners to try again with better evidence (Geist, 2005), the anticipated wave of lawsuits by US-based copyright owners (see Longford, 2007) never materialized.

BMG Canada Inc. v Doe was a dramatic and highly-publicized episode of ISPs stepping up as privacy custodians, with Shaw and TELUS publicly claiming credit for protecting the privacy of their subscribers (G. Shaw, 2004). The decision solidified both the duty of ISPs to protect the identities of their subscribers, and the conditions under which such protection could be overcome in a lawsuit (Knopf, 2013). However, while this particular episode is a good starting point for considering how ISPs developed into the trusted privacy custodians upon which we are all now so dependent (see Kerr & Cameron, 2006, p. 273), it is certainly not the beginning of a straight trajectory through which intermediaries became increasingly-vigorous defenders of subscriber privacy. *BMG Canada Inc. v Doe* was a notable and consequential instance of ISPs

[239] The *Personal Information Protection and Electronic Documents Ac*t (PIPEDA), which was enacted in 2001 and came into effect in stages until 2004.

[240] Who would subsequently become chair of the CRTC (Pitts, 2012).

asserting their positive responsibilities as privacy custodians, but one that was followed by inconsistency, ambivalence, and contradictory attitudes by intermediaries towards the privacy of their users.

In subsequent years, ISPs involved in copyright cases have interpreted their responsibilities as privacy custodians in a variety of ways. When file-sharing lawsuits reappeared in Canada in 2011, the three ISPs involved (Bell, Cogeco, and Vidéotron) did not oppose the copyright owner's attempt to obtain a court order to identify their subscribers (McKenna, 2011; Mediacaster, 2011).[241] In a subsequent case involving the same copyright owner (Voltage Pictures),[242] the ISP (TekSavvy) also did not oppose the court order, but fought for the right to notify the subscribers it was being asked to identify (Dobby, 2012; Gaudrault, 2012b), and argued for ways to minimize the privacy impacts of any information disclosure (TekSavvy, 2015, pp. 722–731).[243] In another file-sharing lawsuit, the ISP Distributel originally agreed to identify some subscribers, but then changed its position and opposed the copyright owner in court, claiming the motion to identify its subscribers would be a threat to their privacy rights

[241] Bell presented its decision as being consistent with privacy protection, stating: “Bell takes the privacy of its customers seriously and always complies with Canadian privacy laws and CRTC privacy regulations. We disclose customer information only when directed to do so by a court order and only to the extent required by such an order. In this instance we do intend to comply with the Quebec Superior Court's order - which relates to less than 10 Bell IP addresses - and have no plans to appeal” (Mediacaster, 2011).

[242] US-based Voltage Pictures has been responsible for some major film productions, but has also been labeled by some as a “copyright troll” because of its multi-defendant file-sharing lawsuits (DeBriyn, 2012). The case involving TekSavvy and Voltage (*Voltage v. John Doe and Jane Doe*, 2014) was unprecedented in Canada due to the number of Jane/John Does the copyright owner sought to identify (with Voltage initially seeking to link some 2,000 IP addresses to subscribers), but was consistent with Voltage's conduct in US courts. Most recently, Rogers has contested a motion from Voltage Pictures to identify its customers, but done so on cost rather than privacy grounds (*Voltage v. John Doe*, 2016).

[243] Ultimately, CIPPIC was granted intervenor status in the case and argued for the privacy interests of subscribers. The court ruled in favor of the motion to disclose subscribers’ identities but imposed a series of conditions intended to limit adverse consequences, including compensation to TekSavvy for the costs of making these identifications (*Voltage v. John Doe and Jane Doe*, 2014; TekSavvy’s compensation became the source of further dispute, see Knopf, 2015).

(Distributel, 2013, pp. 52–54; O'Brien, 2013).[244]

These preceding examples demonstrate how Canadian ISPs operate as privacy custodians in the context of file-sharing lawsuits by copyright owners. In these cases, the negative responsibilities of privacy custodians have been fairly clear and uncontroversial under *PIPEDA*, as requiring a court order prior to any disclosure of personal information. Positive responsibilities have depended more on the discretion of the intermediary, with some choosing to be more assertive than others in defence of users' privacy interests. In contrast, when intermediaries act as privacy custodians in the context of state surveillance efforts, *PIPEDA* has been interpreted as providing greater freedom to disclose information. In these circumstances, negative responsibilities are more easily neutralized by exceptions to the law, giving more latitude to those intermediaries that wish to elevate their roles as state partners above those of privacy custodians. These exceptions to privacy obligations thereby become legitimate justifications for surveillance, and have been key points of contention in the story of 'lawful access' in Canada and debates over the roles and responsibilities of intermediaries.

PIPEDA, lawful access, and exceptions to privacy protection

What is known as 'lawful access' includes a number of positive duties, or requirements for intermediaries to assist state actors in obtaining information or carrying out surveillance. These duties involve complying with court orders, such as those mandating wiretaps (Government of

[244] The change in Distributel's position reportedly resulted from further demands made by the copyright owners (NGN Prima and Riding Films), and from the company's being made aware of what NGN had done with information previously disclosed by Distributel (specifically, NGN had used the information to send the subscribers settlement demands, see O'Brien, 2013). Distributel criticized these practices, as well as the copyright owners' evidence of infringement, stating that "until sufficient evidence is submitted that adheres to the standard required by the Court, Distributel remains the protector if its subscribers' privacy rights" (Distributel, 2013, p. 53). Subsequently to Distributel's opposition, the copyright owners dropped their motion for further disclosure of information (Kyonka, 2013b).

Canada, 2002). A related positive responsibility is the mandatory disclosure of information relating to child pornography (Valiquet, 2011). However, the debate over lawful access has frequently focused on the negative responsibilities of privacy custodians, and the scope of the exceptions to these responsibilities. In other words, an intermediary's responsibilities *not* to disclose personal information can serve as a barrier to lawful access, but one that can often be overcome by state actors through exceptions to privacy law.

The principles underlying *PIPEDA* include consent to the collection and disclosure of personal data, and limiting the collection and the disclosure of data to a specified purpose. The exception to obtaining consent for any disclosure of personal data is where such disclosure takes place “by the authority of law” (OECD, 1980). Therefore, while a prohibition against the disclosure of personal information without consent is a key part of private-sector privacy law in Canada, *PIPEDA* (and related privacy legislation) includes a substantial list of exceptional circumstances in which the non-consensual disclosure of personal information is legally permitted (Lawson & O’Donoghue, 2009, pp. 34–35; Power, 2013, pp. 79–81).

The disclosure of personal information without consent is covered by *PIPEDA*'s section 7(3), which specifies the circumstances in which such disclosures are permissible. These include various kinds of investigations, compliance with court orders, matters of national security, emergency situations, and contacting next-of-kin in instances of injury or death. In these circumstances, information that has been collected by an intermediary for other reasons (such as managing a subscriber's account) can be shared without the knowledge or consent of the subscriber. The most important of these subsections in debates over intermediaries' lawful access responsibilities has been section 7(3)(c.1),[245] which permits disclosure to a "government institution" that has "identified its lawful authority". This section was reportedly introduced into *PIPEDA* "by Industry Canada as a result of representations made by law enforcement and national security agencies. The intent as explained to Parliament was to maintain the status quo for these agencies to allow them to engage in pre-warrant intelligence gathering" (Morin, 2011, p. 4).

Subsequent to enactment, the limits of the "status quo" protected by *PIPEDA*'s "lawful authority" section turned out to be particularly ambiguous (see BCCLA, 2012, pp. 60–61). Eventually, court decisions would provide greater guidance as to how the law should be interpreted, but police agencies and ISPs needed some shared understanding without waiting for these precedents to be established, particularly regarding the important issue of online child pornography (known as internet child exploitation). To this end, the Canadian Coalition Against Internet Child Exploitation (CCAICE) was formed following a 2004 meeting of ISPs, the RCMP, Department of Justice, and the Canadian Centre for Child Protection ("CCAICE," n.d.). The CCAICE went about designing and implementing a protocol that would meet the "intent behind section 7(3)(c.1)" and be "privacy compliant" (Morin, 2011, p. 8). Suzanne Morin (formerly Bell Canada's Assistant General Counsel and Privacy Chief) described (2011) how the protocol for obtaining subscriber information was developed and formalized through discussions between "certain Canadian ISPs, including Bell Canada"[246] and law enforcement organizations,

[245] And in particular, *PIPEDA*'s section 7(3)(c.1)(ii), which permits and organization to "disclose personal information without the knowledge or consent of the individual... [if] the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law".

[246] CCAICE membership in 2005 included most of the major Canadian incumbents as well as industry associations (CCAICE, 2005).

particularly the National Child Exploitation Coordination Centre (NCECC). The protocol was for "a participating ISP, in response to an agreed upon template letter of request, [to] disclose to the requesting LEA [law enforcement agency] the last known name and address of the account holder that was using a particular IP address at a specific date and time" (Morin, 2011, p. 1; see also Public Safety Canada, 2012d, pp. 185–187). This disclosure was "used at the pre-warrant stage of child exploitation investigations only and [was] intended to strike the right balance between ensuring fundamental freedoms and Internet principles, and contributing to eradicating a widely-condemned social evil" (Morin, 2011, p. 1). The protocol began in 2005 as a way for child exploitation investigators in the "pre-warrant" stage to request disclosures that were not "required by law" (not subject to a court order or a specific statutory power). Instead, as per *PIPEDA*'s section 7(3)(c.1), requests for disclosure were based on the police officer's "lawful authority" and the cooperation of ISPs was voluntary.

Along with the new CCAICE protocol for warrantless disclosures, participating ISPs carried out a review of contractual agreements with their subscribers, as a way of providing "additional comfort" that reasonable expectations of privacy were not being violated (Morin, 2011, p. 19). These agreements (including privacy policies and acceptable use policies) explain the responsibilities of an ISP acting as a privacy custodian to its customers, and specify when customers can expect to have their personal information disclosed without consent. Each ISP participating in the CCAICE needed to ensure these policies were compatible with the new warrantless disclosure protocol.

While the CCAICE protocol established a shared interpretation of what *PIPEDA* permitted and what intermediaries would disclose to police on request, it did not preclude other intermediaries from interpreting *PIPEDA*'s section 7(3)(c.1) differently, or adopting a stricter stance as privacy custodians. On the one hand, section 7(3)(c.1) can be seen as an exception to a privacy custodian's negative responsibilities, allowing a company to disclose various kinds of personal information[247] that would otherwise be confidential. But the section can also be read as a complement to these negative responsibilities, where it "arguably operates as a blocking statute", prohibiting voluntary disclosure in cases where police or government agencies have failed to demonstrate their "lawful authority" (Israel, 2012). Because *PIPEDA* does not spell out how an agent of a government institution goes about presenting his or her lawful authority, section 7(3)(c.1) could either be read as an open-ended justification for information sharing, or alternately, as a door that is best left firmly shut by more reticent intermediaries.

Since the phrase "lawful authority" was never clearly defined, it ended up being interpreted in different ways by government agencies and private organizations (D. Fraser, 2011; House of Commons Standing Committee on Access to Information, Privacy and Ethics, 2007; Israel, 2012; Lawson, 2011; Ling, 2014; Morin, 2011; L. Singer, 2012). In some cases, a simple phone call from a police officer requesting information was enough for an intermediary to share

[247] The kinds of "personal information" subject to this section of *PIPEDA* are never specified or delimited, and the law provides no distinction between content and metadata, producing what has been called a "one-size-fits-all" approach (Lawson, 2011). While disclosing the content of a communication was widely interpreted as requiring a warrant, irrespective of section 7(3)(c.1)'s open-endedness, and while the formalized disclosure process between major ISPs and child exploitation policing agencies was limited to name and address information (Morin, 2011, p. 11), it does seem that some companies and government agencies have interpreted the law in a more permissive manner (something CWTA/ITAC expressed concern over in 2011, see Industry Canada, 2014b, p. 28). Reportedly, the RCMP has used this section to request a user's data from a hosting company, Saskatchewan police used it to obtain a French-based file-sharing service's password, and it may have been used by a Canadian national security agency (either CSIS, or CSEC working under Part C of its mandate) to obtain phone data from a UK telecom company (Ling, 2014). The OPC found an RCMP request that sought "user profile information, account creation date and images associated with the user" (Office of the Privacy Commissioner, 2015a, p. 7). Ultimately, since these disclosures are voluntary, it is up to the intermediary to decide whether to comply and how much information to provide. The legal limits of permissible disclosures under *PIPEDA* can only be determined through court cases such as the *Spencer* decision (described below), but individual companies' disclosure practices or perceptions of liability are not necessarily determined by legal precedents.

its records. Other intermediaries set the bar considerably higher, refusing any compromise of user privacy unless mandated by law. For some, this non-disclosure was rooted in an ethical duty to safeguard user privacy to the greatest extent possible,[248] but concerns over the risks of disclosure have apparently also played a part. Lawful access proponents such as the Canadian Association of Chiefs of Police (CACP) and NCECC stated that some intermediaries insisted on court orders for any disclosures because of concerns over corporate liability for privacy violations (House of Commons Standing Committee on Access to Information, Privacy and Ethics, 2007; Public Safety Canada, 2012d, pp. 184, 193).[249] The difficulty of obtaining the cooperation of recalcitrant intermediaries created investigative obstacles and delays, and according to proponents of lawful access legislation, this created a need for revisions to *PIPEDA* which would mandate and standardize compliance (House of Commons Standing Committee on Access to Information, Privacy and Ethics, 2007; Public Safety Canada, 2012d).

Despite several efforts by successive governments, lawful access legislation was never successful in curtailing the discretion of intermediaries to deny some “lawful authority” requests for information. This discretion was largely eliminated by the Supreme Court's *Spencer* decision

[248] There is some indication the community networks, such as FreeNets, might be inclined to take a particularly strong stance as privacy custodians. In 2001 the membership of the Vancouver Community Network resolved “that no information regarding our users or their online activities would be disclosed without a valid court order”, a position the organization emphasized in Public Safety’s 2007 lawful access consultation, when it asserted that any legislation that sought to mandate otherwise would violate Charter rights (Public Safety Canada, 2012d, p. 271). The Executive Director of Ottawa's NCF stated that the organization protects its members' privacy “to the extent that [it’s] legally able”. Prior to the *Spencer* decision, this would have meant insisting on a warrant when PIPEDA would have arguably allowed voluntary disclosure, thereby differentiating NCF from a “regular ISP” (N. Ouzas, personal communication, October 8, 2014). A similar view was stated by a former NCF Executive Director (R. Kouhi, personal communication, October 17, 2014), although neither individual had received a police request for subscriber/member information during his time acting in the position (the NCF had previously received such requests, and responded with a policy of “if you’ve got a warrant, we’ll give you what you’re asking for” (N. Ouzas, personal communication, October 8, 2014).

[249] Lawful access proponents also argued that the concerns of recalcitrant intermediaries were born of “confusion” over what *PIPEDA* entailed, and that new legislation was needed to “clarify” the authority of government institutions (House of Commons Standing Committee on Access to Information, Privacy and Ethics, 2007; Public Safety Canada, 2012d).

in 2014 (*R v. Spencer*, 2014, see Chapter 5), which strengthened privacy custodians' negative responsibilities and effectively barred most voluntary disclosures under *PIPEDA*'s section 7(3)(c.1)(ii). But more than a decade of debate over lawful access and *PIPEDA*'s exceptions demonstrates the role conflict faced by intermediaries serving the needs of government agencies and acting as privacy custodians for their users.

Lawful access and role conflict

The role conflict at the heart of lawful access has been the topic of repeated consultations and public debates in Canada, where surveillance and privacy were often presented as trade-offs. Lawful access proponents rarely made an explicit argument that privacy should be sacrificed in the interests of security, and tended to present lawful access as respecting, protecting or safeguarding privacy rights (Public Safety Canada, 2012d, p. 371; Toews, 2012).[250] However, such claims were frequently accompanied by the metaphor of "balance" – between privacy on the one hand, and what was variously described as security, the needs of law enforcement, public safety, or the public interest on the other.[251] Supporters of lawful access legislation claimed that it struck an appropriate balance (CBC News, 2009; House of Commons Standing Committee on Access to Information, Privacy and Ethics, 2007; Public Safety Canada, 2012d, pp. 183, 187; Toews, 2012), while critics argued that it tipped the scales against privacy (Stoddart et al., 2011), or pointed to the incompatibility of privacy rights and the proposed surveillance measures

[250] This view rested in large part on the legal argument that the metadata subject to warrantless disclosure does "not attract a reasonable expectation of privacy" (Public Safety Canada, 2012d, pp. 331–340, 370). Interestingly, the CACP (2012) also argued that in addition to balancing police powers and privacy rights, lawful access would "enhance" privacy by limiting and increasing accountability for police investigations.

[251] For example, the NCECC's 2007 submission states: "Police understand, value, and respect the importance of protecting individual privacy. We also understand that privacy interests must be balanced with other public interests" (Public Safety Canada, 2012d, p. 183).

(Cavoukian, 2011; Public Safety Canada, 2012d, 2013b, p. 271). The metaphor of balance is often used to frame debates about surveillance and security in a liberal political context, and there are ample reasons to doubt whether security and privacy are somehow exchangeable (Neocleous, 2008, pp. 12–13). However, in Canada's lawful access debate, “balance” became a way of talking about intermediaries' role conflict, wherein companies were expected both to act as privacy custodians and surveillance partners. The limits of what an intermediary could do in one of these roles would end up defining the other.

Until 2014 (pre-*Spencer*), intermediaries were able to resolve their role conflict by claiming compliance with negative privacy responsibilities while voluntarily disclosing personal information, either on an “ad hoc basis” (Public Safety Canada, 2013e, p. 57) or through protocols established between industry and government (Morin, 2011). In other words, the role of an intermediary as a privacy custodian extended only as far as *PIPEDA*'s section 7(3)(c.1)(ii) exception, which granted a great deal of discretion to disclose personal information on request. This latitude included the possibility of denying requests from government, and maintaining the confidentiality of subscriber information. In other words, intermediaries were able to find their own “balance” in this role conflict, and could choose to extend either privacy protection or government cooperation to the legal limit. While uncommon (Public Safety Canada, 2012b, p. 267), refusals to act as willing partners in government surveillance were seen as unacceptable by lawful access proponents, who sought to replace voluntary with mandatory cooperation.

In general, intermediaries have avoided taking a public position on either side of the lawful access debate.[252] Industry representatives have accepted government needs as legitimate, but made their support conditional on having specific concerns addressed (Public Safety Canada,

[252] Exceptions include opposition by Vancouver Free-Net in 2007 (Public Safety Canada, 2012d, p. 271).

2012d, pp. 165, 257). Telecom companies have primarily been interested in clearly determining their obligations under privacy law and lawful access legislation, and wanted to know how legal changes would impact their operations. In other words, the industry's main concerns have been over the costs and obligations of lawful access (Industry Canada, 2014b, pp. 10–30; Nevis Consulting Group, 2003; Paperny, 2012; Public Safety Canada, 2011b), and not over whether lawful access would make them less effective as privacy custodians.[253] It seems that the freedom of individual intermediaries to resolve this role conflict on their own terms would readily be exchanged for legal clarity and financial compensation, and it is only recently that some intermediaries have been publicly asserting themselves as privacy custodians in this debate (see below).

In 2012, the most significant attempt to pass lawful access legislation (as Bill C-30) was widely opposed and proved politically untenable (Ibbitson, 2012), thereby failing to limit intermediaries' discretion. Limitations on intermediary conduct were imposed by the *Spencer* decision (*R v. Spencer*, 2014), which effectively declared most warrantless disclosures to be unconstitutional. This fixed the "balance" of competing roles further in favor of privacy responsibilities than lawful access proponents had hoped. However, even with the restrictive implications of this decision, intermediaries have found novel ways to define themselves as privacy custodians. Additionally, lawful access proponents (unhappy with the implications of *Spencer*) have renewed their push for surveillance capabilities and police powers, giving intermediaries another opportunity to take a public stance on these issues.

[253] For example, during industry consultations in 2002, clarity and costs were the dominant industry concerns, and Vidéotron was the only company that "consistently expressed concerns from a privacy perspective" (Public Safety Canada, 2012d, p. 13).

Redefining privacy custodians through positive responsibilities: Resisting in court, educating the public, and transparency reporting

I have previously described how intermediaries developed as privacy custodians, and some of the different ways that organizations have defined themselves in this role in recent years. The lawful access debate highlighted the inconsistencies among privacy custodians dealing with a longstanding role conflict, and the overwhelming public opposition to Bill C-30 likely convinced some intermediaries of the importance that users attached to privacy. However, the lawful access saga was generally not used by intermediaries to assert themselves as privacy custodians, and privacy interests were primarily represented by other actors in the debate. It is only since the latest lawful access consultation in 2016 that some intermediaries have publicly championed privacy interests (Braga, 2016; Solomon, 2016a, 2016b), but even before this, there are a number of ways in which some intermediaries have recently asserted the privacy of users and redefined themselves as privacy custodians by adopting certain positive responsibilities. I have previously discussed this trend in relation to copyright cases, but recent years provide a number of other noteworthy examples.

As described above, Canadian intermediaries have generally avoided pushing for stronger privacy laws, or (until recently) against weaker privacy obligations. However, some have fought legal battles to assert the rights of their users under the laws which do exist. TELUS and Rogers have both gone to court to argue against police overreach in lawful access (*R. v. TELUS*, 2013; *R. v. Rogers*, 2016). As in the case of *BMG Canada Inc. v Doe*, these companies have rationalized their negative responsibility not to disclose (in the absence of a court order) as a positive responsibility to oppose an improper court order. In both cases, a judge ruled the court order in question to be inappropriate or excessive, but it is important to keep in mind that these instances are not representative of the thousands of court orders that either company annually complies with (*R. v. Rogers*, 2016, paras. 9–10). While rare, these examples of active opposition provide privacy custodians a means of publicly affirming their privacy commitments (Blackburn, 2013; Dobby, 2016a; RogersKevin, 2016), and differentiating themselves from other companies that have presumably complied with similar orders.[254]

In recent years, some intermediaries have also found ways to redefine themselves as privacy custodians without positioning themselves in court. Such efforts include privacy education programs for customers and the broader public, the most notable of which has been the TELUS WISE program, which includes free seminars, school presentations, and online resources (TELUS, n.d.). While TELUS WISE was extended to the public in 2013 (previously available only to business customers), it operates in partnership with MediaSmarts (MediaSmarts, n.d.), a long-standing digital literacy organization that also promotes privacy awareness, and which is partly funded by Shaw, Rogers, Bell, and TELUS.

The 2013 Snowden disclosures prompted a great deal of privacy-related concerns among internet users, giving Canadian intermediaries an opportunity to promote themselves on the basis of privacy and security (Miller, 2014; Woods, 2014). At a Canadian industry conference I attended in 2014, an executive from an incumbent ISP presented the argument that service providers had an opportunity to gain a competitive advantage by offering better security, and showed a photo of Edward Snowden as an answer to the question of why we care about privacy

[254] In the most recent ("tower dump") case involving Rogers and TELUS (*R. v. Rogers*, 2016), these companies were most likely not the only ones to receive such a court order, since police do not appear to have had any indication whether the suspects they were trying to identify were subscribers of a particular company. Geist (2016b) notes that Bell was "conspicuously absent" in the case, and David Fraser (2016) reports that production orders were obtained against six companies, and that only Rogers and TELUS resisted. Rogers has also taken steps to reduce the amount of customer information disclosed in other "tower dump" requests (Rogers, 2016).

and security.[255] In the wake of high-profile data breaches and revelations of sophisticated surveillance programs, many customers have wondered about the extent to which intermediaries are protecting their information. As a result, some privacy custodians have taken proactive steps to improve such safeguards, and to engender trust with consumers by communicating corporate privacy practices.

One of the most significant shifts in recent years toward a more positive role for intermediaries as privacy custodians has been in the form of "transparency reports", and greater disclosure of these companies' role in facilitating state surveillance. Since 2010, a growing number of primarily US-based companies (with Google being the first) have been issuing such transparency reports, documenting how these companies handle requests from both governments and private companies to remove content or disclose information. Canadian intermediaries only began doing likewise after the lawful access controversy had raised considerable questions about the telecom industry's disclosures of personal information, Edward Snowden had heightened concerns over state surveillance, and after inquiries were made by Christopher Parsons and the Citizen Lab (Freeze, Dobby, & Wingrove, 2014; Public Safety Canada, 2014c, pp. 1621–1622). Since 2014, MTS Allstream, Rogers (2014), SaskTel (2014), TekSavvy (2014), TELUS (2014) and WIND have issued such reports (Office of the Privacy Commissioner, 2015c), in some cases despite the role conflict created through contradictory lawful access responsibilities that appeared to restrict such disclosures, including government efforts to limit transparency.[256] However, the

[255] At a separate event in the aftermath of the Snowden disclosures, a cloud service executive remarked that he was "constantly" dealing with institutions that indicated they could not store their data in the United States (Digital Futures Symposium transcript, November 14, 2013).

[256] As companies faced growing pressure to be more open about their role in aiding state surveillance in 2014 (Public Safety Canada, 2014b, p. 1625), some intermediaries expressed concerns that regulations prevented them from disclosing information about lawful access (Kyonka 2014). TELUS first met with government

trend of transparency reporting has reversed in recent years, and only TELUS and Rogers have chosen to continue annual releases, with pressure on transparency issues subsiding since 2014. For now, transparency reports remain an important new positive responsibility, but one that has been neither consistently nor widely practiced.

The future of privacy custodians

While some intermediaries have freely adopted a more positive orientation as privacy custodians, significant changes have also been mandated by recent court decisions that favor stronger privacy protection. The *Spencer* decision now joins a developing body of jurisprudence which recognizes that many kinds of "metadata" are personal information and therefore require privacy protection (Office of the Privacy Commissioner, 2014). More recently, a justice of the Ontario Superior Court ruled that Rogers and TELUS not only had standing to assert the privacy rights of their subscribers in opposition to a court order, but that they are "contractually obligated to do so" (*R. v. Rogers*, 2016, para. 38). For Geist, this represents a "sea change" by affirming that companies have "a positive obligation to defend the privacy interests of their subscribers"

officials in April 2014 "seeking guidance" (Public Safety Canada, 2015a, p. 1) on the sorts of statistical information the company was permitted to disclose (Public Safety Canada, 2014c, p. 1621), but TekSavvy was the first Canadian ISP to publish a transparency report (shortly before Rogers) without consulting government (B. Abramson, personal communication, January 9, 2017). Rogers also did not contact government prior to its June 2014 report, effectively declaring a new approach to privacy and surveillance in which "the needs of [Rogers] customers came first" (Bronskill, 2014). Rogers` Ken Engelhart remarked in an interview that "there was too much sensitivity in the past about not wanting to upset law enforcement officials… We realized we have to get a transparency report out quickly to make our customers satisfied that their information is being dealt with properly" (Freeze, Dobby, & Wingrove, 2014). In the following months, Public Safety and its partner agencies carried out a review and determined that intermediaries could publish transparency reports with aggregated data (Public Safety Canada, 2015a, p.2). In 2015, Industry Canada released guidelines for transparency reports, which included limiting details in such reports "to protect the operational activities and capabilities of Canadian government and law enforcement agencies" (Industry Canada, 2015). Critics called these restrictions "ad-hoc" and "arbitrary" (Karadeglija, 2015b), but Industry Canada's guidelines contributed to the legitimization and standardization of transparency reporting (Parsons, 2017).

(2016b).

However, these trends towards greater privacy protection are countered by legislative currents flowing in the other direction,[257] as well as some intermediaries' efforts to collect and exploit personal information (Fung, 2016). The most notable Canadian example occurred when Bell expanded its collection of personal information in 2013 to include its subscribers' internet browsing habits, as part of an effort to target personalized ads. In response, the company was named in numerous complaints to the Office of the Privacy Commissioner (Henderson, 2014b).[258] The Commissioner found that Bell had not obtained adequate consent from its customers for this collection and use of personal information (Office of the Privacy Commissioner, 2015b), leading the company to withdraw the program and delete the collected information (Dobby, 2015c). In this example, as with a great deal of privacy law, much depends on the question of consent. Intermediaries clearly have incentives to adopt roles as collectors and monetizers of personal information (Fung, 2016). These roles can largely be reconciled with legal obligations by satisfying the requirement for expressed consent, but an intermediary that profits from gathering and exploiting personal information has a qualitatively different relationship with its users than an intermediary that limits the collection of any non-essential information.

As discussed above, intermediaries were largely absent in the public debate over lawful access, with the exception of price concerns and the prospect of passing these costs on to

[257] While case law has shifted towards higher expectations for privacy custodians, particularly in their negative responsibilities around disclosure, legislation in Canada has repeatedly moved in the opposite direction (particularly through Bills C-13 and S-4, see Handa, Birbilas, & Fazio, 2015; Semenova & Wagner, 2014). In the context of case law such as the *Spencer* decision, this has meant that intermediaries can find themselves subject to contradictory duties (Griffin, Simard, & Bellefleur, 2015).

[258] Some of Bell's customers joined a $750 million dollar class-action lawsuit against the company (Boutilier, 2015a). Additionally, Bell's ad program was also the target of a complaint to the CRTC, which was dismissed when the program was withdrawn (Dobby, 2015e).

consumers (Canadian Press, 2012; CBC News, 2009). While it could be argued that it is not the role of intermediaries to advocate for public policies on the basis of privacy concerns, US companies have recurrently taken such positions in the wake of the Snowden disclosures (D. Roberts & Kiss, 2013; Rushe & Lewis, 2013). Such public advocacy also took place in Canada in 2013, but had little to do with limiting government access to personal information. Instead, Rogers, Bell and TELUS lobbied government and appealed to public opinion to prevent Verizon from entering Canada as a competitor. One of their arguments was that the US-based company would be a threat to the privacy of Canadians, and the companies encouraged Canadians to "stand up" and "tell Ottawa" about these concerns (Bell, Rogers, & TELUS, 2013a; Woodhead, 2013). In sum, public policy advocacy is certainly a role that privacy custodians in Canada could adopt in the future, but so far, intermediaries' positive responsibilities have not extended to advocating for public policies to better protect privacy. Instead, when Canadian legislation has enabled greater disclosures of personal information or imposed new surveillance powers, the dominant concerns of the telecom industry have been the costs and technical challenges of implementing these changes.[259]

The future outlook for intermediaries as privacy custodians is therefore quite mixed. Despite some legislative changes to relax negative responsibilities, the *Spencer* decision has restricted voluntary disclosures of personal information to government agencies. With the exception of recently-enacted obligations for companies experiencing a data breach (Lithwick,

[259] Industry concerns over costs and implementation have predominated throughout efforts to enact lawful access legislation, and they also formed the basis of industry's opposition to changes in the Solicitor General's Enforcement Standards (SGES) in 2011 and 2012. Some government officials saw the SGES as an "interim measure" (Public Safety Canada, 2013c, p. 73) and the only regulatory means to compel companies to maintain an interception capacity in the absence of lawful access legislation (Public Safety Canada, 2013c, p. 70). Telecom companies successfully opposed changes to the SGES, primarily on the basis of the costs to meet the proposed lawful interception requirements (Freeze & Trichur, 2013; Public Safety Canada, 2013c, pp. 146–151, 445).

2014a), new positive responsibilities have not been imposed through law. Nevertheless, a number of intermediaries have increasingly adopted a more positive orientation to privacy of their own accord, by asserting the privacy rights of customers in court cases and a public consultation, by issuing transparency reports, and educating the public about the importance of privacy protection. However, such efforts have been wildly inconsistent across the industry, demonstrating the degree of agency and discretion that intermediaries exercise in carving out these new roles (Sargsyan, 2016, pp. 2229–2230). Bell's actions are notable in that the company has failed to pursue a more positive orientation to privacy protection, but also actively pushed in the opposite direction in order to profit from customers' personal information. Despite being rebuffed, the company has stated its plans to attempt a similar program in the future with a revised approach to consent (Dobby, 2015c), and trends in the U.S. (Brodkin, 2015; Chen, 2014; P. Sayer, 2015) suggest that others may follow by making the collection and use of personal information part of their business model. Therefore, it seems reasonable to expect that some Canadian intermediaries will continue to differentiate themselves on the basis of their positive conduct as privacy custodians, while others seek to benefit from their users' personal information and merely maintain compliance with the negative responsibilities of privacy custodians.

The changing roles of privacy custodians

Intermediaries now occupy a pivotal role as privacy custodians. As stewards of information and communications, they are forced to distinguish the privacy status of various data and to apply appropriate protections, but this is by no means a culmination of the hundred-year history outlined earlier in this chapter. There is no coherent governing rationality for privacy custodians beyond what some intermediaries choose to develop internally, with discretion and variability being the defining features of privacy protection in the current milieu.

Public policies to safeguard privacy took time to develop, and did so alongside contradictory needs to monitor conversations, policies to enable state surveillance, and later in relation to copyright surveillance. Relevant legal regimes have sometimes imposed clear obligations and prohibitions, but intermediaries typically exercised a great deal of discretion in determining the nature of their conduct as privacy custodians. This meant making choices about the extent to which information could be collected, used, and disclosed to other parties. Intermediaries are more than rule-bound institutions complying (or failing to comply) with their obligations as privacy custodians. Rather, intermediaries are collective actors that develop their own rationales for what it means to operate as privacy custodians, defining and redefining this role, while resolving the role conflicts that arise when they are subject to contradictory sets of expectations.

I have argued that the responsibilities of privacy custodians can be differentiated as positive and negative expectations. Negative responsibilities, or prohibitions on particular kinds of conduct in the interests of protecting privacy, typically include exceptions that have been at the center of role conflicts, public debates, and court cases involving ISPs. These include *PIPEDA*'s section 7(3)(c.1), which allows for otherwise-prohibited disclosures of personal information, and court orders in copyright cases, which mandate such disclosures. Bell's advertising program violated a privacy custodian's negative responsibilities, since the form of consent that the company relied upon to legitimate its conduct was deemed inadequate.

While privacy custodians have often taken advantage of exceptions to their negative responsibilities, some organizations have been developing new positive responsibilities related to privacy. These include asserting the privacy rights of users in public (court proceedings and a government consultation), educating the public about privacy-enabling practices, and publicly disclosing information through transparency reports. Such efforts allow some intermediaries to distinguish and promote themselves as defenders of their users' interests, or to serve a broader objective of furthering individual autonomy, well-being, and public order (see *BMG Canada Inc. v. John Doe*, 2004, para. 36). While *PIPEDA* requires intermediaries to govern personal information in a way that is aligned with public policy objectives, some intermediaries have gone beyond being compliant instruments of public policy. By doing so, they have essentially taken public policy objectives into their own hands. In some cases, this has meant pushing back against court orders and police demands, or compelling government to draft new policies around information disclosure.

During a period when Canada’s federal government has recurrently moved to weaken privacy protection or promoted information disclosures, the positive orientation of some intermediaries toward privacy governance has been an important counterbalance. But this development should not be overstated, and does not amount to intermediaries strengthening users' privacy rights. Instead, we can see that a limited number of organizations have developed a new kind of practical rationality in regard to privacy, selectively broadening the scope of their actions as privacy custodians beyond their legal obligations. When these actions are aligned with public policy objectives, or when they compel government to draft new policy, we can describe such intermediaries as public policy actors. However, when intermediaries have been consulted on public policies with a significant impact of privacy, as occurred repeatedly on the issue of lawful access, their main concerns have been with costs, challenges of implementation, and the perceptions of their users. Only the most recent (post-Snowden) lawful access consultation saw some intermediaries take a stronger stand in defence of privacy (Braga, 2016; Solomon, 2016a), but it is too early to describe these companies as pro-privacy champions of public policy. Meanwhile, other intermediaries take full advantage of broad exceptions to their negative responsibilities as privacy custodians, and may perceive significant advantages in doing so.

Given such freedom to act, we should expect to see positive contributions by some intermediaries in their roles as privacy custodians, while others govern personal information in the interests of profit and security, seeking merely to remain compliant with their privacy obligations. Assuming that we have a choice of which service providers or networks to use, we (as users or consumers) are left in the position of evaluating relationships with intermediaries on the basis of their privacy practices. Because so many of these practices remain opaque, or are not explained adequately or accurately in stated polices, this ends up being a choice of who we trust as custodians of our personal information. Intermediaries meanwhile, seek to earn or maintain that trust, and those organizations that want to distinguish themselves as good privacy stewards need to be prepared to take an active stand against the pressures that threaten the privacy of their users. Both users and intermediaries are increasingly aware of the importance and value of their relationship with one another, which can either be safeguarded or exploited. Which intermediaries we choose to partner with in this digital dance, is now a choice of great and growing significance.

Chapter 5: Internet service providers as security partners

Historically... there have been few laws needed to compel the cooperation of certain sectors. Unfortunately, in the online world, the sense of a civic duty or public responsibility to assist police, for example with identifying customers, appears to be diminished. The state can no longer count on the voluntary cooperation of certain corporate citizens in the online world to ensure community safety.
-RCMP National Child Exploitation Coordination Centre (NCECC) submission to Public Safety Canada's Customer Name and Address (CNA) Information Consultation, October 2007 (Public Safety Canada, 2012d, p. 182)

As discussed in Chapter 2, it is now widely accepted as self-evident that broadband connectivity is "vital" to society (CRTC, 2016a, paras. 7555–7618). The previously-mentioned consequence of this new truth is that disparities in connectivity have become increasingly consequential. This chapter takes up another problematization, grounded in the assertion that "this same environment for innovation and social interaction has also become a vehicle for those who would do us harm" (Public Safety Canada, 2016, p. 93). As societies have "moved online" (Public Safety Canada, 2016, p. 93), state agencies have become particularly concerned that this new "world... lacks the regimes of law and order that govern our physical world" (Public Safety Canada, 2011a). The drive to secure Canadian society in this new milieu can be seen in a newly assertive role for state agencies, which sometimes seek to compel intermediaries towards these ends. However, state agencies more often attempt to work "collaboratively" by "partnering" with the private companies that own and operate what the federal government has called "Canada's cyber systems" (Public Safety Canada, 2011a).

The previous chapter analyzed the increasingly important role that intermediaries play as privacy custodians. This role developed alongside government requirements for intermediaries to serve as security partners, and privacy is also implicated in a developing set of expectations around cyber security. This chapter will address these security responsibilities in detail, which are becoming increasingly important, albeit in tension with intermediaries' evolving privacy expectations. Both privacy and security are domains of governance where intermediaries exercise considerable discretion. However, unlike privacy, security has been the aim of considerable efforts by the federal government to standardize intermediaries' conduct and expectations. With hundreds of diverse ISPs operating in Canada following liberalization, police agencies have recurrently promoted industry-wide obligations to make these ISPs more consistent and dependable surveillance partners. Cyber security has also been a governmental challenge under regulatory capitalism, with ISPs focused on serving customers who have tended to prioritize costs over security. A number of efforts to regulate ISPs in the interests of security have thus far been unsuccessful, but each new push helps to delineate and renegotiate the role of state agencies in security governance.

There are two types of security programs that have had dramatic implications for Canadian intermediaries in recent years: lawful access and cyber security. As described in the previous chapter, lawful access refers to requirements for intermediaries to assist state actors in obtaining information or carrying out surveillance against persons. Cyber security refers to efforts to protect both networks and persons against various kinds of online threats, and to govern data flows so as to control 'malicious' traffic. In both lawful access and cyber security, government efforts have sought to achieve uniform standards of conduct for intermediaries. For lawful access, this has included longstanding voluntary cooperation between industry and state agencies to fight internet child exploitation,[260] and efforts to mandate lawful access compliance

[260] Through the Canadian Coalition Against Internet Child Exploitation (CCAICE), as discussed in the previous chapter.

through legislation and regulation. Cyber security has taken longer to develop as a government concern in Canadian telecom, and has so far been addressed by mainly through collaborative fora and confidential relationships. These relationships include secret programs disclosed by Edward Snowden, while publicly-acknowledged (albeit little-discussed) "superstructural nodes" (Burris, Drahos & Shearing, 2005) operate to connect government and telecom representatives, coordinate responses to specific incidents, or to work towards long-term strategic objectives.

In this chapter, I am principally interested in the standardization of ISP responsibilities in regard to lawful access and cyber security. While these developments can be understood as an expansion of security and surveillance responsibilities, the more specific ambition is standardization – creating uniformity across time and space through agreed-upon rules, allowing actors to "work together over distance" (see Bowker & Star, 1999, p. 14; Timmermans & Epstein, 2010), and facilitating the coordination of heterogeneous nodes towards some public policy objective. Often, such standardization is less about imposing a new standard for all to meet, and more about bringing some actors in line with a standard already met by others.

As discussed in the previous chapter, privacy and security are deeply interwoven objectives in Canadian telecom, making it impossible to consider one without the other. Contradictory responsibilities of ISPs towards these two ends create role conflicts that intermediaries have a great deal of discretion in resolving. Additionally, some cyber security responsibilities are in conflict with net neutrality expectations. Standardization creates uniformity in an attempt to resolve or stabilize these tensions, but any attempt to legislate compliance risks turning role conflicts into political debates. As a result (and despite repeated attempts at lawful access legislation), standardization in both lawful access and cyber security has largely been achieved through collaboration between government and large intermediaries.[261]

Despite a proliferation of government-industry partnerships and telecom security standards, ISPs' roles as security and surveillance partners are far from standardized, partly because voluntary standards are never uniformly observed, and also because it would be impossible to gain agreement from all of the hundreds of ISPs in Canada. Standardization has certainly not been the outcome for all of the government efforts discussed in this chapter, but it has been rationalized as the means for achieving certain public policy objectives. It is these objectives that are at the heart of this analysis – the surveillance-ready network, ISPs as dependable state partners, 'clean' internet traffic, and the nation's cyber security. In the long term, further standardization for ISPs security responsibilities may be inevitable, and would be much easier to achieve if cooperation from the few largest incumbents was all that was necessary. But for now, efforts at standardization can help us understand the policy demands of state actors and the role conflicts these create for ISPs.

This chapter makes a chronological argument, documenting how security concerns have expanded from individual subscribers and users (lawful access) to governing internet traffic (cyber security). Initially, widespread internet adoption led state agencies to demand surveillance access to packet-switched networks through analogies to telephone (circuit-switched) networks. Lawful access standards also had to deal with the internet-era problem of identifying individuals through digital traces – particularly on the basis of IP addresses. As lawful access standards were being developed collaboratively with the telecom industry, and alongside several attempts to legislate and regulate lawful access, ISPs increasingly began governing internet traffic to meet

[261] Although lawful access procedures have also been shaped by court decisions (see Chapter 4) that have limited ISPs' discretion in some practices.

their own security needs.

Lawful access ultimately targets the body, attempting to uncover the person behind the IP address, or collecting information about individuals that might be used against them. In contrast, cyber security deals with traffic and its circulation. This distinction can be related to the shift from discipline to security in Foucault's writing, with security (of the eighteenth-century urban environment) being concerned with “organizing circulation, eliminating its dangerous elements, making a division between good and bad circulation, and maximizing the good circulation by diminishing the bad” (Foucault, 2007, p. 18). As the diversity, scale and severity of cyber security threats increased, standardization has been pursued as one solution to the problem of 'bad circulation' (typically referred to as 'malicious traffic'). While lawful access standards deal with meeting state surveillance needs, directed at individual users or subscribers, cyber security standards deal with ensuring ISPs are surveilling their networks appropriately, and taking certain actions in response to threatening or unusual traffic. These projects are by no means independent, and lawful access is sometimes now listed under the broader category of cyber security, but the important trend is the growing involvement of ISPs in monitoring and discriminating amongst internet traffic.

Lawful access: Interception and disclosure responsibilities

The standardization of lawful access was achieved relatively late in the history of telephone networks, but the emergence of ISPs brought a new set of challenges. As previously discussed, electronic surveillance in Canada had gone from being largely unregulated before 1974, to a formalized regime of legal authorization and criminal penalties. But according to police and government spokespersons in the early 2000s, internet technologies left this legal regime in the dust. The law would have to 'catch up', or police would 'lose' key investigative tools. Lawful access was not promoted as a new investigative capability enabled by digital networks, but instead as a vital tool that police had come to depend on in the telephone era, and which was now under threat from new technologies and new kinds of intermediaries. Lawful access advocates claimed they were attempting to "maintain" their traditional powers during these times of change (Government of Canada, 2002, p. 5). To this end, ISPs were asked to accept new requirements to assist law enforcement and national security agencies, and these requirements would be standardized across an industry that now included a very diverse cast of companies. Lawful access was meant to turn these intermediaries into a consistent and dependable set of instruments in the fight against crime and national security threats.[262]

Beginning in the early 2000s, efforts to develop or "update" lawful access in Canada passed through several stages,[263] multiple different versions of legislation,[264] informed by numerous "stakeholder" consultations,[265] behind-the-scenes meetings, and public debates. For much of this period, lawful access requirements encompassed two kinds of standardization and

[262] While police were the most prominent public advocates for lawful access, internal and public documents justified lawful access as a vital tool for both law enforcement and national security agencies (specifically CSIS, see CSIS, 2012 on how lawful access serves the agency's operational needs).

[263] According to Shaw and Valiquet's (2012), Legislative Summary of Bill C-30, law enforcement agencies had called for legislation to require "all telecommunications service providers to have technical means in place to enable police services to carry out lawful interceptions on their networks" since 1995 (p. 3). However, federal governments only began pursuing lawful access as part of the policy agenda beginning in the 2000s.

[264] The number varies depending on what legislation is considered under this category. Dedicated lawful access Bills include C-50, C-51, and C-52 in 2010; and 2012's Bill C-30, none of which were successfully enacted. However, recently enacted Bills C-12 (Israel, 2012; Lawson, 2011; L. Singer, 2012) and C-13 (Forcese, 2013; Geist, 2013b) both had lawful access implications.

[265] Unlike the copyright consultations, the first lawful access consultations (held in 2002, 2005 and 2007) were largely closed to the public. Instead, the public's "stake" was represented by a variety of groups and individuals, including advocates for civil liberties, privacy, consumers, victims of crime (Public Safety Canada, 2012d). The 2007 consultation was opened to the public for a short period following criticism in news media about its closed nature (CBC News, 2007; Parsons, 2015a, p. 265; Public Safety Canada, 2012d, p. 128), while the most recent was part of a broader public consultation on national security in 2016 (Braga, 2016).

their attendant responsibilities. The first was a “design standard” (Timmermans & Epstein, 2010, p. 72), specifying the surveillance capabilities of telecom networks. Known as the “interception component” (Public Safety Canada, 2012d, p. 142) of lawful access, these standards would require intermediaries to have an “interception capability” built into their networks. Without this power, police or CSIS might find that an intermediary did not have the capability to wiretap a subscriber, even under court order. In a 2007 Ministerial briefing, Public Safety Canada (PS) claimed that these circumstances required government to negotiate with intermediaries and pay for intercept capabilities, creating situations that “can take years” to resolve (Public Safety Canada, 2012d, p. 142).[266] Furthermore, PS claimed that some intermediaries “refuse to cooperate, or charge a premium for assistance,” and these “gaps” in capability were known to criminals and terrorists (Public Safety Canada, 2012d, p. 142). The solution would be to mandate that intermediaries install and maintain surveillance equipment, or implement particular surveillance capacities on request. Proposed responsibilities under Bill C-30 also included that intermediaries open their networks to government inspections, testing, and that they identify employees involved in interceptions (Geist, 2012a; House of Commons of Canada, 2012).

The second set of lawful access responsibilities was a “procedural standard” (Timmermans & Epstein, 2010, p. 72), which would impose uniformity in how intermediaries disclosed what was alternately called “basic subscriber information” (BSI), or “customer name and address” (CNA) information. This entailed the creation of a mandatory disclosure regime for “discrete identifiers” such as subscriber names, phone numbers, IP and street addresses (Public

[266] In a document from 2012, the example used by PS to justify the need for interception capabilities involves a Hell's Angels case in which it took the RCMP six weeks to develop a “solution” for an intermediary that was unequipped for interception – a period during which “vital evidence was not collected” (Public Safety Canada, 2014b, p. 1152).

Safety Canada, 2015a, p. 1), when these were requested by state agencies.[267] The need for uniform access to subscriber information was articulated in greatest depth and detail by the RCMP's National Child Exploitation Coordination Centre (NCECC). Among lawful access proponents, the NCECC provided some of the only statistics and examples to justify new obligations for ISPs, and was cited by the RCMP as detailing the problems that "Canadian police in general face in obtaining basic, non-sensitive customer information" (Public Safety Canada, 2012d, p. 364). In its October 2007 submission to a Public Safety Canada consultation, the NCECC explained what was known to police as the "CNA problem" (Public Safety Canada, 2012d, p. 182):

> In the past telephone companies were the traditional source of customer name and address information for police. They voluntarily assisted by providing basic name and address information to identify customers using their services. Today certain companies as well as Internet Service Providers (ISPs) resist and regularly refuse to assist in this way. For these companies this change may be due in part to legal obligations they have had since 2000 to protect the privacy of their customers' personal information, confusion over the "lawful authority" of police to request this type of non-sensitive customer information without first obtaining a warrant, and their desire to avoid potential litigation and corporate liability for alleged privacy violations. As a result, police now find themselves asking federal lawmakers to contemplate enacting laws compelling these companies to provide this basic customer identifying information to police.

The excerpt given above includes a number of recurring justifications cited by proponents of lawful access (see House of Commons Standing Committee on Access to Information, Privacy

[267] Lawful access proponents typically emphasized the limited nature of such data as a way to minimize concerns over the impact of its disclosure on privacy (Public Safety Canada, 2012d, p. 187), likening BSI/CNA to "phone book" information (Public Safety Canada, 2012d, p. 194). However, it should be noted that the category of BSI/CNA information has included various kinds of identifiers in different iterations of lawful access legislation. At one point, proposed lawful access powers encompassed eleven distinct kinds of subscriber information. This raised substantial criticisms of the government's "phone book" analogy, including concerns that individuals could be identified and tracked through their devices as they went about their daily lives, or when they attended events such as protests (Cavoukian, 2011; Geist, 2012a; Parsons, 2011, 2012). In the immediate aftermath of these criticisms, the federal government introduced bill C-30, which reduced the number of identifiers from eleven to six (E. Shaw & Valiquet, 2012).

and Ethics, 2007), and some attendant tensions around the issues. First, the NCECC notes that the relationship between telcos and police has traditionally been a cooperative one. The NCECC claims that (as of 2007) this relationship no longer holds true for some ISPs,[268] and that some smaller intermediaries[269] seem to be playing by different rules and making unreasonable demands of police investigators. Five ISPs in particular “constantly refuse to cooperate” (Public Safety Canada, 2012d, p. 186), and “a few small ISPs openly advertise their lack of cooperation with police to attract customers” (Public Safety Canada, 2012d, p. 185).[270] The RCMP (through the NCECC) therefore promoted lawful access legislation to “clarify the responsibilities ISPs have to provide basic customer identifying information to police upon request” (Public Safety Canada, 2012d, p. 193). This “clarification” would have the effect of transforming ISPs’ voluntary cooperation[271] into a legal obligation. A mandatory, uniform process for information disclosure would eliminate the possibility of intermediaries interpreting their roles as privacy custodians in such a way as to obstruct police investigations.[272]

[268] Elsewhere in the same document, the NCECC also alleges that mobile phone companies are “increasingly reluctant to cooperate” (Public Safety Canada, 2012d, p. 192).

[269] While the NCECC does distinguish small, problematic ISPs from more cooperative “major telephone companies” (Public Safety Canada, 2012d, p. 192), elsewhere in its 2007 submission the organization cites statistics that indicate “33% of NCECC requests produce unsuccessful results”, including “refusals, lack of response and insufficient data retention times” (Public Safety Canada, 2012d, p. 197). Such a high proportion of “non-compliance” suggests a broader problem than a few bad actors, and could be a result of incumbents not collecting and retaining data in a desired fashion. The NCECC's figures from 2010 show a “CNA not provided” rate of 27.5%, with 18.2% due to data not being available (Public Safety Canada, 2012b, p. 267).

[270] Besides the bad actors accused of being uncooperative for financial gain, the other reasons identified by the NCECC for the ISP industry’s resistance include intermediaries’ legal obligations as privacy custodians, and their fear of liability for disclosure of subscriber information (Public Safety Canada, 2012d, pp. 191–192).

[271] Which the NCECC characterized as an “obligation” even under the voluntary regime (Public Safety Canada, 2012d, p. 193).

[272] In one case cited by the NCECC, a police officer had his phone stolen, and the telephone company “refused to provide information about calls made on the customer’s stolen phone after the theft”, because “it was concerned about protecting the privacy interests (the calling records) of the alleged thief” (Public Safety Canada, 2012d, p. 193).

Government-industry collaboration on lawful access

Intermediaries were not passive targets of proposed lawful access legislation, raising various concerns and playing different roles throughout the lawful access saga (Parsons, 2015a). Many companies worried about the consequences of an expanded set of responsibilities for ISPs, and some became actively involved in meetings, such as the *Collaborative Forum on Lawful Access Issues* (Public Safety Canada, 2014b, pp. 1162–1163, 1257),[273] to craft lawful access policies. Industry concerns over lawful access included safeguarding subscriber privacy and the fear of being seen as agents of the state (Industry Canada, 2012, p. 4, 2014b, p. 25), but companies have been primarily interested in determining the details of what would be required of them, how easily they could meet these obligations, and the costs of complying with new obligations.[274]

Government-industry collaboration gave some intermediaries privileged access to information about the government's plans and a channel for communicating their views, creating what Geist (Geist, 2012b) called a "two-tier" policy approach, where "secrecy and backroom industry talks" shaped surveillance policies before these were announced to the broader public. But while the relationship between Canadian intermediaries and government never turned

[273] Formally established in early 2012 during the introduction of Bill C-30, the *Forum* built on government-industry relationships established in previous years (Industry Canada, 2014b, p. 10) and worked alongside a "ITAC/CWTA Lawful Access group" (Public Safety Canada, 2014b, p. 1194) in reviewing the legislation.

[274] Specific concerns included questions around the sorts of equipment intermediaries would be required to purchase, install, and operate, what sorts of information they would be required to collect about their subscribers, and how quickly they would be forced to provide such information upon request (Industry Canada, 2014b, pp. 10–30; Nevis Consulting Group, 2003, Chapter 4; Paperny, 2012; Public Safety Canada, 2012d, p. 3, 2014b, pp. 952–953). The costs of lawful access include time commitments by ISP employees dedicated to processing law enforcement requests, and the purchase of specialized equipment to meet government demands. These costs raised persistent questions as to whether they would be paid by ISPs, police, or perhaps even through "proceeds of crime" (Industry Canada, 2012, pp. 2, 241, 349). Intermediaries involved in the initial round of lawful access consultations in 2002 were broadly sympathetic to the government's objectives, and even indicated a willingness "to absorb some costs for public safety", but emphasized that "these costs must be kept to a minimum" (Public Safety Canada, 2012d, p. 12).

adversarial during the development of lawful access policies, the telecom industry was also never a full partner in the process, and its concerns were not necessarily addressed by government. Federal governments were inconsistent in seeking industry input on various proposals as lawful access legislation was being drafted, leaving some intermediaries to argue that the industry was not being adequately consulted (CSIS, 2012, p. 1). Some meetings were organized at the request of intermediaries (Industry Canada, 2014b, p. 10; Public Safety Canada, 2014b, p. 222), who were keen to establish collaborative relationships and receive details of proposed legislation well in advance so that there would be "no surprises" (Industry Canada, 2014b, p. 25). While extensive discussions and meetings between industry and government took place behind closed doors (Geist, 2012b; Paperny, 2012), not all intermediaries were equally represented in government consultations, with incumbents having the greatest involvement (Industry Canada, 2014b, p. 10; Public Safety Canada, 2012d, pp. 9–11, 77).[275]

As different versions of lawful access legislation were being drafted and discussed, voluntary cooperation and collaboration continued under the existing legal regime, such as CCAICE's BSI disclosure protocol (see Chapter 4). By and large, incumbents cooperated with police and maintained the surveillance capabilities the government sought to mandate. However, consistency remained a problem and even a single uncooperative ISP could limit the reach of state agencies.

Forging consistency among privacy custodians

While an uncooperative intermediary could simply be forced to disclose information with

[275] Smaller intermediaries often lack the resources to participate in government consultations and proceedings, or do so through an industry association such as CAIP (Canadian Association of Internet Providers), and more recently, through CNOC.

a court order, lawful access proponents argued that obtaining court orders for the sorts of information routinely requested by police would either be too onerous or impossible.[276] One approach to resolving this issue would have been to clarify just what is meant by "lawful authority" in *PIPEDA* (see Chapter 4), or to provide immunity for companies disclosing personal information to government agencies.[277] But while some non-cooperation may have been based in intermediaries' fear of liability, the more fundamental problem from the perspective of lawful access advocates was the voluntary nature of disclosures made under section 7(3)(c.1).[278] A voluntary system, without standardized processes or a universal set of obligations, created "an inconsistent, ad-hoc approach" (Public Safety Canada, 2012d, p. 143). As long as the disclosure of personal information involves the discretion of intermediaries, there is the possibility that some companies will refuse to cooperate. Therefore, the policy solution pursued through successive iterations of lawful access legislation was to make the disclosure of subscriber information mandatory. Instead of allowing intermediaries to define their roles as privacy custodians under the flexibility of *PIPEDA* and their company privacy policies, lawful access advocates sought to impose consistent obligations throughout the telecom industry.

The problem of inconsistency among privacy custodians in the telecom industry was often presented as a consequence of liberalization, which had resulted in a diversity of intermediaries of various sizes and with differing approaches to dealing with law enforcement

[276] Court orders take time to obtain and drain police resources. In some cases, it is simply impossible to obtain a warrant at the preliminary stages of an investigation, where there are insufficient grounds to believe that a criminal offence has been committed. Access to subscriber information has frequently been presented as being key to these "pre-warrant" stages of an investigation, but as long as intermediaries have no legal obligation to comply, "police depend on moral suasion and a service provider's sense of civic duty to obtain their cooperation" (Public Safety Canada, 2012d, p. 190).

[277] Indeed, some legislative steps in these directions were taken in 2011 and 2012, but never concluded (Israel, 2012; L. Singer, 2012).

[278] For example, and RCMP presentation slide from 2009 introducing the CNA problem is titled "Problem with the Status Quo is Reliance on Voluntary Cooperation" (Public Safety Canada, 2013f, p. 87).

(Government of Canada, 2002, p. 4; Public Safety Canada, 2013f, p. 85). Some of these "mom and pop" ISPs operated with limited resources that made compliance with lawful access obligations an onerous burden, while other small intermediaries were alleged to be actively facilitating illegal activity, existing "solely to trade in child sexual abuse" (House of Commons Standing Committee on Access to Information, Privacy and Ethics, 2007). The lack of cooperation by some small ISPs and the fear that that these intermediaries would become safe havens for criminal activity was recurrently raised by lawful access proponents, while incumbents were generally recognized to be cooperative with police investigations (Bailey, 2007; Public Safety Canada, 2012b, p. 267). Incumbent ISPs already participated in CCAICE, had procedures in place for handling lawful access requests on a "routine basis", and maintained dedicated staff[279] for these purposes (Public Safety Canada, 2012d, p. 164). Small ISPs on the other hand, often had little or no experience assisting police investigations, and faced the greatest impact in installing and maintaining interception capabilities – the cost of which threatened to put some companies out of business (Arellano, 2011; Canadian Press, 2012; Industry Canada, 2012, pp. 2–3; Public Safety Canada, 2012d, p. 155; Solomon, 2011).

Lawful access legislation was intended to standardize responsibilities that most of the ISP industry had already accepted, since incumbents generally already maintained wiretap capabilities and disclosed subscriber information on request. However, it would not be fair to say that small ISPs were true targets of lawful access proposals, since incumbents would also be forced to modify their disclosure practices, or face clear penalties for failing to meet certain standards. Before liberalization, police could depend on a relationship with a single telecom

[279] In 2009, Bell Canada reportedly had twelve employees dedicated to supporting law enforcement, processing an average of 250,000 law enforcement requests a year (J. Brown, 2009).

provider in a given area (Hubbard, Magotiaux, & Proestos, 2002, pp. 362–363), but some police departments were now paying large monthly bills to multiple incumbents for surveillance services that often had no regulated rates.[280] Lawful access proponents were therefore keen to subject all intermediaries to a common regime, and ISPs of all sizes were acutely interested how lawful access would affect the costs of doing business, and what changes to their operations would be required. Even where proposed obligations were already largely being met by intermediaries through voluntary cooperation, new legislation would have the effect of standardizing methods, procedures, and equipment, along with attend obligations to monitor and enforce compliance with these obligations.[281]

Standardization through jurisprudence

Successive federal governments failed to enact dedicated lawful legislation during the period between 2000 and 2015 due to a lack of commitment, the contentiousness of surveillance

[280] Whitaker (2012, p. 341) argues that once they lost their monopoly status, incumbents began seeing state actors as customers and shifting the costs of surveillance to the public sector – even building a profit margin into the fulfillment of government requests. I see no evidence that ISPs have sought to profit from lawful access, although the sums paid for their surveillance services were often substantial. Recently, the RCMP and Rogers have been at odds after the company imposed new fees for certain court-ordered kinds of surveillance, which the RCMP refused to pay, threatening Rogers with criminal charges if the company demanded payment before providing the services. Responding to the controversy, the Canadian Association of Chiefs of Police (CACP) argued that “police services throughout Canada should not be required to bear the costs associated with court-ordered activities,” and that Rogers should “bear the reasonable burdens of compliance with such orders as part of its general corporate responsibility to the community" (Bronskill, 2015a). While in many cases intermediaries disclose information without charge, RCMP documents indicate that millions of dollars must have been paid by police to telecom companies since the early 2000s, with address information (name, street address, email) costing between $1 and $15 per disclosure, call record disclosures running into the hundreds of dollars, and in excess of a thousand dollars per wiretap (Ling, 2015).

[281] Bill C-30 would have empowered government-appointed “inspectors” who had the authority to examine the facilities and equipment of a telecommunications service provider, including any relevant documents, to verify compliance with the act (House of Commons of Canada, 2012, secs. 33–38; Public Safety Canada, 2014b, pp. 662–664). According to a 2013 government memo, telecom companies argued against the need for such a law by stating that “the telecommunications market will soon shift to a point where interception capability will simply become a standard component of available equipment” due to a worldwide “proliferation of interception capability legislation and standards” (Public Safety Canada, 2013d).

and privacy issues, and (particularly during the Bill C-30 controversy in 2012) the inability of the federal government to make a persuasive case for lawful access (Parsons, 2015a; Whitaker, 2012).[282] Ultimately, greater consistency in the handling of warantless requests for information would come about not through legislation to mandate cooperation, but a court decision to prohibit this sort of "invisible handshake" (Birnhack & Elkin-Koren, 2003).

The 2014 Supreme Court of Canada's unanimous decision in *R. v. Spencer* (2014) ruled that the voluntary disclosure of subscriber information by an ISP in a Saskatchewan child pornography case could not be justified by *PIPEDA*'s section 7(3)(c.1), because such a disclosure to a government institution violated section 8 of the *Charter* and thereby amounted to a warantless "search" (Lithwick, 2014b).[283] Since a legal precedent does not necessarily or immediately translate into a change in policy, the *Spencer* decision did not result in all government agencies suddenly ceasing to request subscriber information (Boutilier & McLeod, 2014; Ling, 2015),[284] and subsequent legislation continued to presume the legitimacy of some

[282] An attempt to revise the Solicitor General's Enforcement Standards to mandate lawful access also failed in this period following resistance from the telecom industry, see note 259.

[283] In other words, identifying oneself as a police officer involved in an investigation and citing *PIPEDA*'s section 7(3)(c.1)(ii) was not sufficient grounds to obtain information subject to a reasonable expectation of privacy (and the court found that subscriber information linked to an IP address was indeed subject to a reasonable expectation of privacy). The Court concluded that "lawful authority" must mean something more than a "simple request" by police, and that such authority was not granted by *PIPEDA* (*R v. Spencer*, 2014, paras. 70–71). The decision was also interesting in that it distinguished between three "distinct although overlapping" kinds of "informational privacy", namely privacy as secrecy, privacy as control, and privacy as anonymity (*R v. Spencer*, 2014, para. 38). The Court recognized the anonymity was a particularly relevant privacy concern in the context of internet usage and subscriber information, and that the identification of a subscriber through an IP address engaged significant privacy interests. Additionally, the decision may have significant implications for the privacy policies of intermediaries and reasonable expectations of privacy in regard to these policies (which as previously stated, inform the subscriber that their personal information may be disclosed in a variety of circumstances). In response to the argument that the defendant had no reasonable expectation of privacy in his personal information given the contents of the intermediary's (Shaw's) Joint Terms of Service, Privacy Policy and Acceptable Use Policy (which can be considered contractual agreements), the court found that "the contractual provisions, read as a whole, are confusing and equivocal in terms of their impact on a user's reasonable expectation of privacy" (*R v. Spencer*, 2014, para. 60).

[284] According to the *Spencer* ruling, voluntary disclosure is still widely permissible in a range of circumstances, including where there is no reasonable expectation of privacy, "exigent" or emergency situations, or the

such disclosures.[285] Without additional clarification or a new legal regime for warrantless disclosures, the *Spencer* decision still remained open to some competing interpretations. As with the tower-dump decision discussed in the previous chapter (*R. v. Rogers*, 2016), intermediaries were left in the position of assessing the constitutionality of legal demands before agreeing to comply and determining what kinds of disclosures violated their users' "reasonable expectation of privacy" (Therrien, 2015). However, a clear implication of the *Spencer* decision was that many of the millions of voluntary disclosures by intermediaries since the early 2000s (see Office of the Privacy Commissioner, 2015a) had been unconstitutional. According to the Supreme Court, such disclosures were in fact prohibited by *PIPEDA*, rather than being enabled by the law's exceptions in section 7(3)(c.1). As a result, the routine disclosure of personal information by intermediaries to police underwent a massive change during the summer of 2014, with companies largely ceasing to comply with non-emergency "pre-warrant" requests and some reflecting this change in their privacy policies (Bronskill, 2015b; Dobby, 2014b; TELUS, 2014).[286]

The police response to this new standard of privacy protection was to argue that their jobs had become more difficult, and as a result society had become less safe.[287] The post-*Spencer*

prevention of "imminent bodily harm" (*R v. Spencer*, 2014, para. 74).

[285] Following the *Spencer* ruling, cyberbullying legislation was enacted that provided greater immunity for intermediaries voluntarily disclosing information in certain circumstances, and amendments to *PIPEDA* were criticized for expanding the scope of voluntary disclosures to non-state organizations (Geist, 2014b; Lithwick, 2014a, pp. 12–13; Therrien, 2015; Wingrove, 2014).

[286] TekSavvy (2014) made a similar change in the months prior to the *Spencer* ruling as part of an internal privacy policy review.

[287] Whereas previously, subscriber information could typically be obtained the same day as requested, police now estimated that applying for a court order could add days (Payton, 2014) or weeks (Bronskill, 2015b) to the process. According to one internal RCMP survey, the effect this has had on police investigations has not been significantly negative, mostly resulting "in investigative delays, but not necessarily derailing investigations or changing ultimate outcomes" (Boutilier, 2015b). Publicly, police claimed the *Spencer* decision has meant that some criminal investigations are not being pursued, with the head of the Toronto Police Sex Crimes Unit claiming that the number of children rescued has been "cut in half" as a result of the decision (Cribb &

requirement for police to obtain a court order for subscriber information certainly means that the process takes more time, effort, and is limited to situations that would satisfy a judge.[288] There have since been repeated calls by police advocates for warantless access to subscriber information (Bronskill, 2015b; Geist, 2017), but as things stand, intermediaries' responsibilities as privacy custodians trump the discretion they once exercised as surveillance collaborators.

To summarize the above, lawful access legislation was an attempt to standardize ISPs' conduct in a way that resolved the role conflict discussed in the previous chapter, but the most powerful means of shaping lawful access have been collaborative fora and court decisions. In contrast, the federal government has largely avoided the legislative route in its work to standardize cyber security,[289] where court challenges have also been less likely to arise. This is because the primary security and surveillance actors are ISPs themselves, eliminating the possibility of conflict between industry privacy custodians and state agencies, as seen in the tower-dump decision (*R. v. Rogers*, 2016). Additionally, while lawful access targets individuals who may be prosecuted and challenge the validity of these measures in court, cyber security generally targets internet traffic through technical means and avoids use of the courts.

The rise of cyber security

On the one hand, developments in both lawful access and cyber security are part of a

Greenblatt, 2015). TELUS has recently “collaborated with law enforcement agencies to establish a new process to expedite the sharing of this critical information through court orders where children are in danger, while abiding by the spirit and language of the Spencer decision” (TELUS, 2016a, p. 132).

[288] Specifically, that police had a “reasonable belief” an offence had been committed and evidence would be found as a result of the search (Hubbard et al., 2015, Chapter 3). Bill C-13 changed the legal standard for obtaining metadata (“transmission data”) to a lower “reasonable suspicion” standard (Forcese, 2013) in 2014, but it is unclear what effect this has had on police requests for subscriber information.

[289] An exception being Bill S-4 in 2014, which imposed certain obligations for organization that had experienced a data breach (Lithwick, 2014a).

gradually unfolding “securitization” of the internet around the world (Barnard-Wills & Ashenden, 2012; Deibert & Rohozinski, 2010; Dunn Cavelty, 2013; Hansen & Nissenbaum, 2009; Zajko, 2015), wherein state agencies are increasingly asserting themselves through internet policy and responsibilizing intermediaries to deal with particular threats.[290] But cyber security in particular also encompasses a broader set of concerns that echo an earlier conception of security, rooted in European urbanization and the problem of managing the circulation of a town's “mobile elements” (Foucault, 2007, p. 20). Whereas eighteenth-century planners proposed ways to arrange the movement of people, animals, and goods through the town, while maintaining surveillance and hygiene within the city walls (Foucault, 2007, pp. 20–21), today's concerns are with positioning “cyber sensors” in telecom infrastructure and maintaining network hygiene (CSEC, 2011a). Security was a major preoccupation for eighteenth-century political theorists, as “a set of expectations concerning the undisturbed development of the life processes of society” (Neocleous, 2008, p. 29). As Neocleous (2000, 2008) argues, these expectations came to be associated with the protection of private property and the smooth operation of the market mechanism underpinning the liberal order.

Twentieth-century notions of 'national security', developed during the Cold War, seemed to prioritize the protection of the state and its interests (Neocleous, 2000). However, in Canada as in the United States (which have a shared discourse of national security, see Kinsman, Buse, & Steedman, 2000, p. 281), the security of the economy and state were inseparable, particularly

[290] Here, securitization refers to processes through which grave and existential “cyber” threats are identified and addressed, often entailing a “return of the state” (Bendrath, 2007; Deibert & Rohozinski, 2010, p. 30) to internet governance. While many authors (frequently identified with the Copenhagen School of security studies) focus on how visible political actors make 'securitizing moves' by identifying existential threats and proposing solutions, I have argued that the expansion of cyber security in Canada has largely been a technocratic project quietly carried out by security professionals (Zajko, 2015).

given the threat posed to both by communism. While global capitalism no longer faces such an existential threat, national security remains closely tied to safeguarding economic assets.[291] As described in Chapter 1, Canada's federal government and the CRTC have often described the importance of internet connectivity by using the language of "the digital economy" (CRTC, 2015c; Government of Canada, 2016). Canada's assemblage of cyber security programs are rationalized as protecting the digital economy against its existential threats – attacks against "critical infrastructure" (CSTAC, 2013; Public Safety Canada, 2011a) and strategic hacking by state-sponsored "Advanced Persistent Threats" (APTs, see Zajko, 2015).

For Canada's federal government, the link between national and cyber security is explicit. In June 2013, Public Safety Canada reconfigured its National Security Branch as the National *and* Cyber Security Branch. The change was meant to address "the need for a seamless approach to cyber and national security... [and] the increasing importance of cyber security as a Government of Canada priority" (Public Safety Canada, 2014d). But as with eighteenth-century conceptions of security, cyber security also encompasses much more mundane concerns over traffic flows and network hygiene. 'Infected' computers become a cyber security concern when these are linked together (as botnets) to flood networks with 'malicious' traffic. Technical interventions can control some of this activity, but cyber security is often presented as "primarily a people issue", that requires "getting people to adopt better cyber hygiene practices" through "public awareness, education, and engagement" (Public Safety Canada, 2016, p. 110).

Much of what currently falls under the heading of cyber security has long been addressed (particularly by the private sector), as information, computer, and network security (or IT

[291] While national security and economic prosperity are not synonymous, they are often presented as complementary in the discourse of government agencies such as CCIRC (see Public Safety Canada, 2016, p. 39).

[information technology] security).[292] However, cyber security encompasses a broader set of concerns, and its discourse operates by tying these diverse elements together. The project of cyber security ties personal responsibility to national interests, private partners with state agencies, and addresses a growing array of threats and social problems. Therefore, while the development of cyber security in Canada (as in the US) can be seen as the combination of the technical concerns of IT security with the goals of national security (see Nissenbaum, 2005), it is better understood as linking IT security with collective referent objects, such as "society", ' 'the nation' ', and ' 'the economy" (Hansen & Nissenbaum, 2009). Rather than simply privileging the security of the nation-state, cyber security ties networks, organizations and individuals to societal and political referent objects. Cyber security is a collective endeavor and a unifying project. It is often linked to the traditional goals of national security, but also encompasses a broader set of social and ethical concerns (von Solms & van Niekerk, 2013), and "gains its coherence from making connections between referent objects" (Hansen & Nissenbaum, 2009, p. 1163).[293]

While lawful access is largely concerned with the problem of identifying, locating, and monitoring individuals (in 'meatspace') on the basis of digital records, cyber security typically operates at the level of internet traffic – detecting, filtering, re-routing, and manipulating data packets. Lawful access serves state surveillance needs, particularly for crime control, but also including a variety of governmental functions for which telecom-derived information might be

[292] It should be noted that in the private sector, IT security and cyber security are often treated as synonymous and used interchangeably (von Solms & van Niekerk, 2013). While cyber security can refer to everything that has traditionally been covered by IT security, it also has a much broader usage, particularly by state agencies – which is the focus of this chapter.

[293] This unifying discourse is exemplified by the presentation given by the Deputy Minister of Public Safety to representatives of the private sector at first meeting of CSTAC (described later in this chapter). Competing telecom companies participating in the cyber security partnership were presented as having a "shared interest... in ensuring that individual Canadians and Canadian businesses trust our infrastructure, our products, services and institutions" (Industry Canada, 2014a, p. 61). Participants were then told that, "it only makes sense to work together to keep our telecommunications infrastructure reliable, resilient and trusted. It benefits us all" (p. 65).

useful. Cyber security, on the other hand, is divided amongst referents: It encompasses both state and private-sector strategies to secure networks against network-scale threats,[294] as well as programs to protect individual users of the network from individually-targeted threats.[295] In addition to technical interventions, government agencies and private industry have implemented educational programs to promote safer conduct among users. In other words, cyber security covers an expansive and growing set of concerns, and may even include lawful access as part of its overall strategy, as *Canada's Cyber Security Strategy* (Public Safety Canada, 2011a) does.

While the pivotal internet surveillance debates in Canada have thus far concerned lawful access, the critical issues of the future pertain to the larger category of cyber security. Cyber security is the advancing frontier of intermediary governance over data flows, transforming ISPs away from the ideal of a ‘dumb pipe’ (that simply carries traffic) and towards intelligent networks that maintain network hygiene and protect against cyber threats. In addition to its traditionally defensive focus on protecting information and networks, the pursuit of cyber security has expanded to include moral and legal conduct by internet users, for instance in regard to cyberbullying (Cabinet Office, 2011; Government of Canada, 2015). Additionally, some intelligence agencies (including Canada’s closest Five Eyes allies, see Perlroth, Larson, & Shane, 2013) have been compromising technologies, weakening IT security, covertly penetrating networks, and rationalizing such actions as a way to further cyber security. [296] Finally, cyber

[294] Such as distributed denial-of-service (DDoS) attacks.

[295] Most commonly, these are attacks that do not seek to compromise a specific machine, but are carried out with the objective of compromising as many individual machines as possible.

[296] While cyber security (as practiced by ISPs), has traditionally entailed a defensive posture against threats, some cyber security practitioners have advocated for a more offensive posture (Maurer, 2012), and Canada's CSE has apparently been merging its defensive and offensive capabilities (CSEC, 2011a). Offensive techniques include counter-attacks, pre-emptive operations, and compromising other networks to gain intelligence. While ISPs would face legal liability for carrying out these sorts of operations, attacks by Canadian government actors would necessarily traverse private networks, and would have to be permitted through in order to be effective.

security now also encompasses lawful access, and its attendant political debates about privacy and surveillance.

Intermediaries as gatekeepers: From child pornography and spam to cyber security

A significant reason why the last attempt to pass comprehensive lawful access legislation failed in 2012 was the response Public Safety Minister Vic Toews received when he attempted to use the stigma against child pornography to gain support for the government's bill. Instead of mobilizing support, he faced a public backlash from Canadians who were angry at his suggestion that opposing the bill meant "standing with" child pornographers (Public Safety Canada, 2013b).[297] While the strong response elicited by the topic of child pornography was badly managed by the government's introduction of the *Protecting Children from Internet Predators Act* (C-30), the seriousness of the issue had already spurred Canadian ISPs into action in 2006. In addition to the CCAICE protocol for disclosure of subscriber information discussed in the previous chapter, incumbents also agreed to block access to web sites that had been identified as hosting child pornography under CCAICE's Cleanfeed Canada initiative. This was justified as an attempt to "make the Internet safer for Canadians and their families by reducing their chances of accidentally coming across images of child sexual exploitation on the Internet" (Cybertip.ca, 2006).[298] In a country with an otherwise 'open' internet, blocking access to web content was only

When this happens, the ISP's infrastructure becomes "a weapons platform" (D. McMahon & Macaulay, 2010, p. 26) for state agencies. These developments and the resulting conflicts between defensive and offensive operations are beyond the scope of this dissertation, and are more of an issue for state institutions than ISPs.

[297] Toews's statement was a response to a question posed by Liberal MP Francis Scarpaleggia in the House of Commons, who was told he could "either stand with us or with the child pornographers" (House of Commons, 2012). Toews's remarks contributed to the "overwhelmingly negative" (Public Safety Canada, 2014b, p. 637) media coverage of the Bill after its introduction, and subsequent correspondence from the public to the government about Bill C-30 was highly critical and often angry (Public Safety Canada, 2013b)

[298] Modeled after a similar UK project, Cleanfeed works through a blocklist of URLs compiled by CCAICE and

acceptable given the nature of child pornography, which few would argue should be protected by some idea of 'net neutrality'. Through this limited action against the most universally-despised kind of internet traffic, Canadian ISPs became gatekeepers rather than mere conduits, and faced no opposition in doing so.

Mueller calls the “child safety movement” the “vanguard of Internet content regulation” (2010, p. 190), with its rationale for website blocking based on the universal criminalization and condemnation of child pornography. However, programs like Cleanfeed joined even earlier efforts by ISPs to use blocklists for filtering flows of malicious traffic that directly harmed users or affected how these networks operated. ISPs have long worked independently and collaboratively to block spam and phishing e-mails (Mueller, 2010, pp. 163–172), and filter traffic associated with denial-of-service attacks (Geng & Whinston, 2000). Today, these traffic management processes have continued to develop; ISPs are becoming increasingly involved in governing digital flows to and from their users, as actors in the expanding domain of cyber security.

In becoming agents of cyber security, ISPs are transforming themselves away from the model of a 'dumb pipe', or mere conduit that simply carries traffic (thereby avoiding any responsibility for the contents of the pipe), and towards that of a 'smart pipe' that detects and 'cleans' internet traffic of threats. Some Canadian ISPs have long acted as security providers by offering such services to government and business clients (see Scalet, 2007), but a broader shift is underway in which these practices are increasingly applied to the network as a whole. In the process, ISPs move further away from the ideal of net neutrality and the end-to-end principle, where discriminating between data is prohibited, and towards a world where discrimination is the

distributed to incumbent ISPs, who implement it automatically.

norm. ISPs are expected to monitor activity on their networks, as a basis for actionable intelligence – knowledge used to control traffic. The role conflict this creates is between common carrier or net neutrality expectations for ISPs to treat all traffic equally, and towards the expectation that ISPs manage traffic according to whether or not it is classified as a cyber threat. But it is also a prime example of the trend towards intermediation at the heart of this dissertation, in which ISPs become ever-more active agents, governing connectivity towards an expanding list of ends.

Governing cyber security in Canada

Mapping all of the different agents involved in Canada's cyber security is beyond the scope of this chapter, but as in much of the rest of the world, securing telecom infrastructure and internet traffic is primarily the responsibility of the owners and operators of telecom networks. Officially, the role of government is to secure government networks, help coordinate private actors and facilitate information-sharing. Since Canada’s Communications Security Establishment (CSE) is a member of the international security alliance known as the Five Eyes (Cox, 2012; NSA, 2013), some materials relating to the agency’s secret conduct have also been revealed through Edward Snowden's documents. These show examples of how CSE gains access to internet traffic through “special source operations” (CSEC, 2009, 2010, 2011a, 2011b, 2012a, 2012b; Wark, 2016), involving one or more Canadian telecom industry partners. However, unlike the “special source” relationships in the US (NSA, 2009), these documents give us little insight into the basis of Canadian partnerships, so I will devote the rest of this chapter to the security partnerships with private industry that are openly acknowledged (although little-publicized) by the federal government.[299]

Recent years have seen a proliferation of industry-government cyber security associations in Canada, emphasizing various forms of information-sharing and standardization.[300] These are what Burris et al. (2005) conceptualize as “superstructural nodes”, operating as “nodal assemblages” (p. 43) or nodes that connect “representatives of different nodal organizations… to concentrate the members’ resources and technologies for a common purpose but without integrating the various networks” (p. 38). In regard to ISPs, the most important such organizations are the Canadian Cyber Incident Response Centre (CCIRC), the Canadian Telecommunications Cyber Protection Working Group (CTCP), and the Canadian Security Telecommunications Advisory Committee (CSTAC). While these organizations either include or maintain relationships with police and national security agencies, none have the authority to compel ISPs to behave in certain ways. Instead, they rely on the voluntary cooperation of their members to address threats to a common interest.

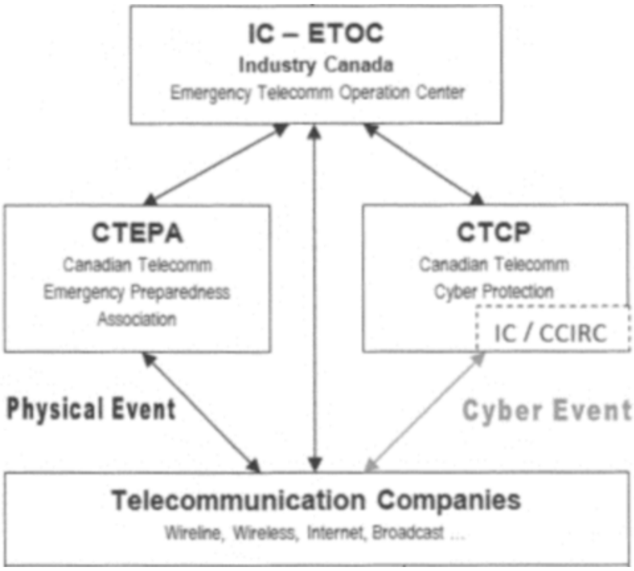
Of these, CCIRC (part of Public Safety Canada) acts as Canada’s national Computer Emergency Readiness Team (CERT). It was formed in 2005 as one of the first federal government efforts to deal with cyber security, and following some high-profile security failures, now operates with increased resources and a narrowed mandate oriented largely towards the

[299] The public visibility of the relationships discussed in this section has been subject to some internal debate. For example, the release of the *Best Practices* prepared by CTCP and CSTAC (described below) was initially meant to be publicized during Cyber Security Awareness Month in October 2013 (see Industry Canada, 2014a). In the end, government opted for a “low-profile” approach to the release of the document, which included the “public acknowledgement” of CSTAC's existence (ISED, 2016, p. 228), albeit with only “cursory information” about the group (p. 250). Apparently, it is important that intermediaries are aware of the existence of such collaborative relationships and that these efforts also undergo “public disclosure” (p. 251), but generally the public visibility of these security partnership has been carefully limited.

[300] These include the Canadian Telecommunications Emergency Preparedness Association (CTEPA, see Leafloor, 2004, p. 9), the National Cyber-Forensics and Training Alliance (NCFTA, see http://www.ncfta.ca/) and the Cyber Security Threat Exchange (CCTX, see https://cctx.ca/), as well as the Information Technology Association of Canada's (ITAC) Cyber Security Forum (https://itac.ca/csf/).

private sector (Office of the Auditor General of Canada, 2012).[301] CCIRC solicits information about cyber threats, analyzes malware, distributes a variety of regular reports to its private sector 'partners' or 'clients', establishes and disseminates guidelines, helps coordinate the response to significant threats, and impels organizations to act when threats are identified within their networks. For instance, if a foreign actor discovers malicious traffic originating from a Canadian network, they may notify CCIRC, which in turn will notify the Canadian ISP and assist in mitigation or help to coordinate filtering (Public Safety Canada, 2012a, pp. 2055–2057, 2012c, pp. 1719–1720, 2014a, p. 2260).

Figure 3 – CCIRC/CTCP Relationships and Role when Responding to a "Cyber Event"[302]



[301] For government networks, this role is played by CSE's Cyber Threat Evaluation Center (CTEC) and the Government of Canada Cyber Incident Response Center (GC-CIRT) in Shared Service Canada, both of which collaborate with CCIRC (CSEC, 2014, pp. 54–57). CCIRC prioritizes threats to critical infrastructure and does not have the resources to notify "Joe Public" of cyber threats (Public Safety Canada, 2014a, p. 1297)

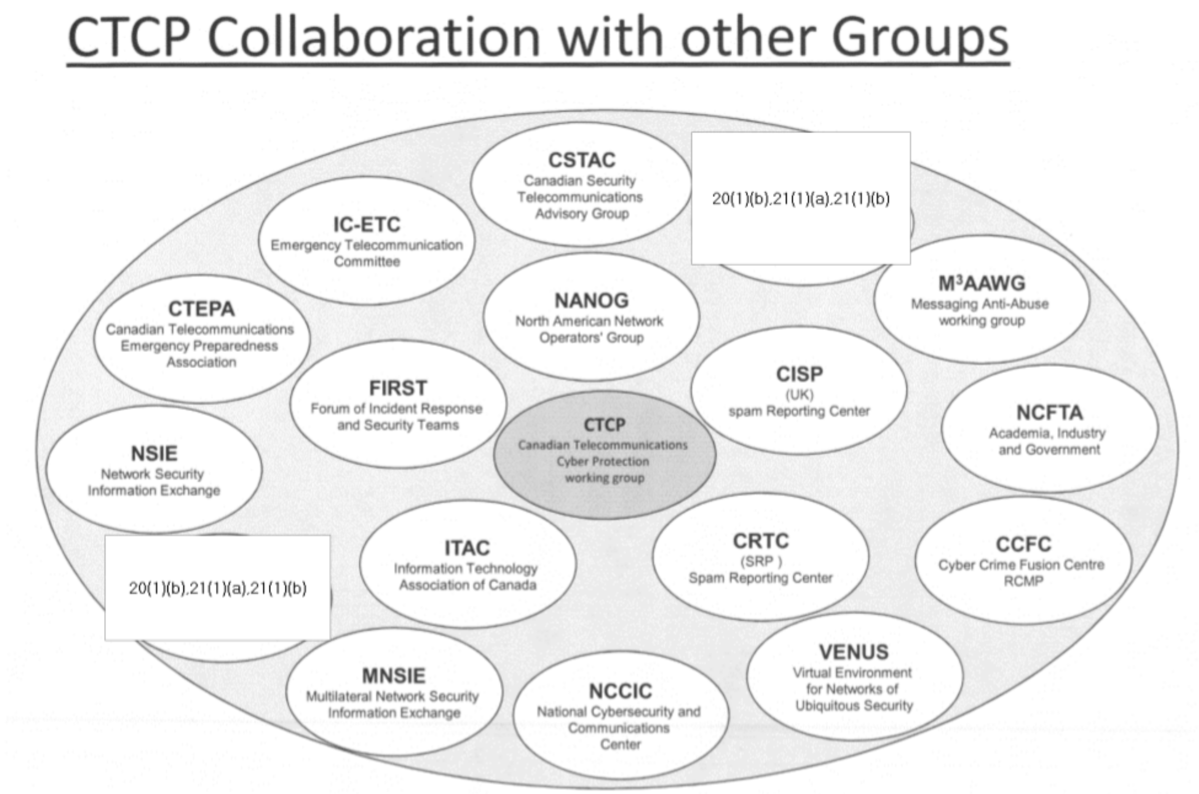
[302] Although CCIRC now deals largely with threats on private Canadian networks, it maintains relationships with both private industry and other government departments. This image from 2014 shows the "cyber incident response flow", involving a response from CCIRC and CTCP to a specific event (ISED, 2016, p. 73). Both organizations can also serve to link ISPs and their cyber security incidents to other relevant government agencies (Figure 4 below).

CTCP (established in 2003), is a longstanding partnership between government and industry that acts as an "operational group" (CSTAC, 2013), collaborating and sharing information over email, a web portal, and weekly teleconferences (ISED, 2016, p. 156). CTCP 'liases' with a large number of other cyber security groups (see Figure 4 below), works closely with CCIRC in responding to particular incidents (see Figure 3 above), and (since 2010) helps CSTAC achieve its objectives. CTCP is a government-industry association that has been chaired/co-chaired by Industry Canada (now ISED).[303] Its private-sector membership is limited to companies and individuals that meet specific requirements (ISED, 2016, pp. 53–61; Public Safety Canada, 2015b, p. 173), namely as operators of "critical infrastructure" (CSTAC, 2013). Members include IT security managers of major ISPs (Leafloor, 2004, p. 5), along with representatives from Public Safety, the military, RCMP, CSIS and CSE (ISED, 2016, p. 156). The relationships maintained under the auspices of CTCP can be activated as an "emergency response" capacity (Public Safety Canada, 2013g, p. 1018) and to coordinate actions against specific cyber threats as these arise (see Public Safety Canada, 2012c, pp. 138, 1556, 1698). CTCP has also worked with CSTAC on more long-term and strategic projects, such as information-sharing and standardization (Industry Canada, 2013, 2014a). Since the same companies are often represented in both associations, CTCP representatives report to CSTAC, implement CSTAC recommendations (CSTAC, 2013), and may be "tasked" by an ISP's CSTAC representative to assist with CSTAC projects (Industry Canada, 2014a, p. 105).[304]

[303] CTCP's organization and relationships have been progressively formalized in recent years, and in January 2015 a new "Management Committee" was created with three industry and government representatives (with Industry Canada joined by CSE and CCIRC), to meet once a year to review membership, member conduct, new projects and activities, and funding (ISED, 2016, pp. 6–7).

[304] However, CTCP can also "propose its own work projects for approval to the CSTAC" (Public Safety Canada, 2015b, p. 156).

Figure 4 – CTCP's Collaborative Relationships[305]


CTCP Collaboration with other Groups
CSTAC
Canadian Security Telecommunications Advisory Group
20(1)(b),21(1)(a),21(1)(b)
IC-ETC
Emergency Telecommunication Committee
NANOG
North American Network Operators' Group
M³AAWG
Messaging Anti-Abuse working group
CTEPA
Canadian Telecommunications Emergency Preparedness Association
FIRST
Forum of Incident Response and Security Teams
CISP
(UK)
spam Reporting Center
CTCP
Canadian Telecommunications Cyber Protection working group
NCFTA
Academia, Industry and Government
NSIE
Network Security Information Exchange
20(1)(b),21(1)(a),21(1)(b)
ITAC
Information Technology Association of Canada
CRTC
(SRP)
Spam Reporting Center
CCFC
Cyber Crime Fusion Centre RCMP
VENUS
Virtual Environment for Networks of Ubiquitous Security
MNSIE
Multilateral Network Security Information Exchange
NCCIC
National Cybersecurity and Communications Center

CSTAC was established in November 2010 for the purposes of high-level information sharing[306] and strategic collaboration between the telecom industry and government. Where the focus of CTCP is on an operational level, CSTAC provides strategic guidance to CTCP,[307] and acts as a "senior point of contact" between industry and government (Industry Canada, 2014a, p. 89). It is co-chaired by government (Industry Canada/ISED)[308] and an industry representative, with private-sector membership composed of senior executives responsible for technology and

[305] CTCP works with a variety of Canadian and international government agencies, industry associations, and collaborative fora, two of which have been redacted in this figure (ISED, 2016, p. 77).

[306] CSTAC participants must obtain Secret security clearance so that they can receive classified briefings by government (Industry Canada, 2014a).

[307] CTCP and CTEPA are sometimes listed as CSTAC's "working level committees" (ISED, 2016, p. 45).

[308] Initially, Public Safety Canada was to act as a government co-chair alongside Industry Canada (Industry Canada, 2014a).

security (such as a company’s Chief Technology Officer or Chief Technical Officer).

Modeled on similar partnership 'committees' in the US and UK, CSTAC was justified within government as a way to better understand telecom network vulnerabilities and the telecom industry's ability to address various threats (Industry Canada, 2014a, p. 11). As a collaborative forum, CSTAC was intended to be a way for “industry to contribute to government policy”, but it was also imagined that government would use it as an “opportunity to contribute to industry network security policies and procedures” (Industry Canada, 2014a, p. 1).[309] Specifically, this meant the group would collaboratively work towards standardizing cyber security.

As one of its first tasks in 2011, CSTAC (working largely through CTCP) went about establishing a “Cyber Security Standard for Telecommunications Service Providers” (Industry Canada, 2014a). An initial formulation (at a time when Bell was CSTAC’s industry co-chair, see Houle, 2016)[310] was dubbed the “National Clean Pipe Standard” (D. McMahon, 2011). This represented an attempt to formalize and legitimate the role of ISPs as providers of “network hygiene”. While the standard that ultimately emerged from CSTAC (2013) was more general, and did not include any certification or compliance mechanisms, the dream of the 'clean pipe' remains an important vision for the future of connectivity and the role of ISPs as security providers.

[309] At the first CSTAC meeting, these objectives were presented in terms that empowered industry: “To promote the telecommunications industry view of protective security matters with Government... To influence the evolution of policy, regulation and legislation... [and] to provide advice to GoC on matters of national security” (Industry Canada, 2014a, p. 89).

[310] CSTAC's industry co-chair position was meant to have a tenure of one year before changing hands, although finding new volunteers for the position has not always been easy (Public Safety Canada, 2015b, p. 166).

Standardizing network hygiene

In North America, cleanliness and hygiene have become common metaphors to describe ISPs' expanded role in cyber security. One document prepared for the Deputy Ministers Committee on Cyber Security,[311] described maintaining network hygiene as “regularly performing the 'bread and butter' activities of network and information technology (IT) security” (Public Safety Canada, 2013a, p. 22), such as updating access privileges, applying security-related patches (Public Safety Canada, 2013g, pp. 133–134), operating intrusion detection systems, and educating users (Public Safety Canada, 2013a, p. 31). While maintaining hygiene can refer to routine IT security work, the term also has a more specific usage in regard to 'cleaning' internet traffic.

Mary Douglas's (1966) explanation of the relationship between hygiene and social order is well-known, but this particular pursuit of social order – the “clean and safe” internet (Scalet, 2007) – can only be achieved through continuous surveillance. This is because the best way to achieve “clean” pipes is for an ISP to build “intelligence” into the network (making the pipes “smart”). This is to say, an ISP needs to monitor internet traffic, discriminate between acceptable and undesirable traffic and have a way of dealing with the latter.[312] Ideally, these interventions are largely automated, with equipment inspecting and categorizing data packets or monitoring

[311] “DM Cyber” first met in January 2012, and is composed of some of the most high-ranking bureaucrats from government departments with a security role (the Deputy Minister of Public Safety, National Defence, Foreign Affairs, Industry Canada, as well as the heads of CSIS, CSEC and the RCMP, and several others). Its role is to “establish policy direction; set priorities; monitor progress on the implementation of *Canada's Cyber Security Strategy*; and consider emerging issues” (Public Safety Canada, 2013a, p. 19).

[312] A former Bell executive describes this process as relying on “upstream intelligence” (UI), or “information about specific Internet protocol addresses (IPs), domains and Autonomous System Numbers (ASNs) behaving in manners indicative of threats... UI quantitatively identifies IPs, domains, and ASNs, which threaten online assets... UI is a source of information available beyond the [local network] perimeter up into the carrier networks that form the bedrock of the Internet, and a place typically considered 'no man’s land'” (Macaulay, 2010, p. 22).

and categorizing flows of traffic, applying set criteria to detect the malicious or unusual. Traffic flagged in this fashion can then receive special treatment from routers and servers, such as blocking, 'throttling' or 'blackholing'.

These techniques are routine for large ISPs, which use them to manage network disruptions caused by attacks, to “recover” the large amounts bandwidth associated with malicious traffic (Macaulay, 2010, p. 22), to reduce customer complaints, and prevent the reputational harms of being a network that either enables or is successfully disrupted by attacks (Eeten & Bauer, 2008). ISPs have long offered security services to their 'enterprise' and institutional customers, such as businesses and public-sector organizations who can configure these systems to their preferences. ISPs have an advantage over other network security providers because of the visibility they enjoy into their entire network, allowing them to identify and predict threats on the basis of broader patterns of activity (Dickson, 2015). In the future, ISPs will continue to develop security programs along both lines: as a core component of their networks, and as a “value-added service” (Standing Senate Committee on Legal and Constitutional Affairs, 2009) for those customers willing to pay. How ISPs practice cyber security has been left largely to their discretion, but as with lawful access, efforts have been underway to standardize what will increasingly be seen as a core responsibility. Standardization also becomes a way of neutralizing cyber security's key role conflicts with other responsibilities – namely privacy and net neutrality.

Individual standards relevant to cyber security have been developed internationally through standards-making organizations such as the ISO and IETF. Some of these have in turn been integrated into voluntary or compulsory standards developed at the national level (see

CSTAC, 2013). Canadian federal agencies have been much more inclined to forge voluntary cyber security standards and govern through superstructural nodes than to compel compliance. CCIRC for instance, has no power to compel standardization from ISPs, but it does develop "best practice guidelines" for securing systems and mitigating specific attacks (CCIRC, 2016). Similarly, what began as CSTAC's *Cyber Security Standard for Telecommunications Services Providers*, became the *Security Best Practices for Canadian Telecommunications Service Providers* (CSTAC, 2013), a change in terminology meant to better reflect the "voluntary nature" of these standards (Industry Canada, 2014a, p. 136).

As with two components of lawful access (interception capabilities and access to subscriber information), cyber security includes design standards that govern the equipment used by ISPs, as well as procedural standards for how these institutions operate. CSTAC's (2013) *Best Practices* deal mostly with the latter, but ISPs must operate specialized hardware and software to meet some of these procedural standards. For instance, ISPs should be able to monitor network traffic for "anomalies" and "threat indicators" (CSTAC, 2013, sec. 4), and have the capability to "throttle, filter, and block" categories of "malicious or inappropriate traffic" (CSTAC, 2013, sec. 5). Other *Best Practices* are strictly procedural and deal with social responsibilities of ISPs. These include participating in industry and government information-sharing processes (CSTAC, 2013, sec. 6), and notifying subscribers when the ISP "becomes aware of a security breach or malware that is affecting a customer's computer, whether as a victim of an attack or as the perpetrator of an attack" (CSTAC, 2013, sec. 5.2.1).

While cyber security now has an abundance of standards, these have not yet produced much uniformity among the conduct of Canadian ISPs.[313] However, my argument is not that cyber security is successfully being standardized in Canada, but rather that these standards can inform us about the evolving role that ISPs are playing in society as security providers, and the role conflicts that result.

ISPs as providers of cyber security

The evolving role of ISPs as security providers can be seen in the development of CSTAC's cyber security standards/best practices (CSTAC, 2013; D. McMahon, 2011), and the related discourses promoting "clean pipes", "secure pipes", "smart pipes" (Dickson, 2015) and "upstream intelligence" (Macaulay, 2010). These sources can tell us about the transformation that has been underway as ISPs take an increasingly active role in monitoring and policing internet traffic, and the role conflicts that must be reconciled as ISPs move further in the direction of acting as security providers. First, it is important to further understand market pressures for and against security services.

As previously mentioned, the idea of "clean pipes" is not new, and ISPs have been offering such services for many years (Scalet, 2007). Furthermore, governments around the world have long been trying to regulate or mandate traffic filtering (often described as censorship) by ISPs, justifying such measures as furthering public safety or maintaining social order (Deibert, Palfrey, Rohozinski, & Zittrain, 2008, 2010, 2012). Private companies selling surveillance and filtering products have marketed these to governments and ISPs using the

[313] A voluntary ISP Code of Conduct, following the Australian model (see note 314), was proposed within Industry Canada in 2012 (Industry Canada, 2013, p. 24), was presented to representatives of major ISPs in 2013 (Geist, 2013a), but was ultimately abandoned by government.

language of clean pipes and cyber security (Sandvine, 2016; Trilling, 2000).[314] However, security professionals have long remarked that the threats against which they defend are under-appreciated by individuals and institutions.

Convincing clients (or senior management) of security's value is an ongoing struggle in the IT security industry. If security is included or offered as a service by an ISP, clients will often choose to do without it (or demand its removal) if this results in lower rates. Because of the low value many clients have traditionally placed on security, private-sector competition can undermine security, as the pursuit of lower prices results in a “race to the bottom” where “security often gets left behind” (Macaulay, 2015; also D. McMahon, personal communication, November 21, 2012). As with other undesirable consequences of marketization addressed in earlier chapters, this is a problem that can potentially be addressed through standardization and regulatory compliance, bringing security up to a higher level “where [the] market will not drive it” (Standing Senate Committee on National Security and Defence, 2012).[315]

However, even in a market where some ISPs may neglect security to keep prices down or attract certain customers, the pressures mentioned in the previous section (to reduce costs related to poor security) have led most major ISPs to implement security measures well beyond their legal obligations. As ISPs take a more active role in cyber security, they rapidly encounter role conflicts, particularly when security services are deployed across an ISP's entire network. From a

[314] In particular, Australia has worked with ISPs to implement a voluntary code of conduct to address cyber threats affecting the public (Hilvert, 2010), and longstanding efforts to regulate filtering or to provide a “clean feed” of the internet to the public (Pyburne & Jolly, 2014). Australia is a close (Five Eyes) ally of Canada, and its efforts are sometimes cited (or “leveraged”) by Canadian agencies (CSTAC, 2013). In 2011 Public Safety Canada discussed with its Five Eyes the possibility of establishing “international norms and standards for conduct in cyberspace” (Public Safety Canada, 2014a, p. 231).

[315] A technology lawyer recently argued that without cyber security standards, it becomes difficult to advise clients about the level of security they should maintain. Without standards to “point to”, security is determined by “negotiation between the customer and the supplier” (Taddese, 2016).

regulatory perspective, there is nothing wrong with ISPs carrying out surveillance or filtering to meet a subscriber's expectations. If a business or a school board wants their ISP to filter certain kinds of traffic, whether for reasons of safety, confidentiality, or productivity, then that is their choice. It is when such interventions are extended to “the general public”[316] that they potentially conflict with ISPs' responsibilities as privacy custodians and with public expectations of net neutrality.

Cyber security and privacy

The relationship between cyber security and privacy is complex, reflecting the many dimensions of both. Some forms of information security are synonymous with some kinds of privacy, when they are both concerned with limiting access and maintaining the confidentiality of information. Surveillance may be used to monitor traffic into and out of a network (including the conduct of individuals using the network), but all of this might be done to ensure that private information residing within a network remains private. However, just because cyber security can complement or enhance privacy does not eliminate the tension between the two responsibilities.

In the example of individuals being surveilled so as to protect information on the network, the tension is between the privacy of the individual and the need to keep information (such as confidential business information) private. Communicating this tension is complicated

[316] As described by David McMahon (representing ITAC) before a Senate Committee, and answering a question about the security responsibilities of ISPs: “Net neutrality and privacy issues also come into play. People want to be able to go places, download things, visit sites and so on. There is a limit to what restrictive security policies any carrier can uniformly put on the Canadian public. A bank, for instance, may have very stringent policies that we can put in place, and their networks can be a lot cleaner. The same goes for any particular enterprise. However, when you are providing bandwidth for the general public, you are riding a fine line as to how much security you provide without impinging upon people's privacy issues and providing their ability to operate on the Internet, and get themselves infected in a lot of cases” (Standing Senate Committee on Legal and Constitutional Affairs, 2009).

by the fact that the language of privacy and security is often ambiguous, making it unclear what dimension of privacy or security is being discussed, or whether these two are complementary or contradictory. For example, two Canadian security professionals writing about ISPs' role in cyber security state that "In most cases, privacy enhances security. However, too much freedom and lack of security controls, in the name of privacy, actually backfires, and destroys privacy" (D. McMahon & Macaulay, 2010, p. 24). McMahon and Macaulay claim that the appropriate "balance between content examination... and privacy" is largely "settled in jurisprudence" (2010, p. 25), but in regard to cyber security, this balance is currently tilted in favor of surveillance powers. Certainly, there are privacy considerations when personal information is collected for cyber security (CSTAC, 2013, sec. 8),[317] and CSTAC's *Best Practices* were revised prior to release due to input from the Office of the Privacy Commissioner (Public Safety Canada, 2015b, p. 236). However, the CRTC has granted very broad latitude for traffic monitoring and management as long as these are "employed to protect users from network threats... as a necessary part of an ISP's network operations" (CRTC, 2009b, sec. 44). ISPs can accommodate privacy custodian responsibilities by limiting surveillance and the collection of information to what is necessary to provide cyber security, but expectations around net neutrality can present a thornier kind of role conflict.

Smart pipes, dumb pipes, and net neutrality

The practical rationality required of a future-oriented ISP is that of a smart pipe. This means that in addition to all of the roles and responsibilities discussed in this and previous

[317] CSTAC's *Best Practices* explicitly recognize that privacy laws "take full precedence over the guidelines listed" (CSTAC, 2013, sec. 8).

chapters, ISPs now have the capability to directly discriminate among types of internet traffic, and this capability is promoted as the key to their future. The surveillance technologies that enable the smart pipe are not new, and have been used to categorize and govern traffic towards various ends for many years. But the development of smart pipes has been driven by cyber security, which is also the most accepted regulatory justification for ISPs engaging in 'traffic management'. However, even in cyber security, there is a fundamental role conflict between the ISP acting as a smart pipe and the principles of "net neutrality" (Wu, 2003). While the need for security has thus far largely been privileged over net neutrality, the expansive potential of cyber security (Zajko, 2015) and the transformation of ISPs into smart pipes means there is a strong potential for conflict over just what kinds of surveillance and discrimination is legitimate.

A former Security Liaison Officer at Bell recently stated that "the nightmare scenario for a carrier is to be a dumb pipe, and just carry the internet traffic, and add no value to it" (Macaulay, 2015). While the 'dumb pipe' is just a conduit for packets, the smart pipe is an actor – its intelligence is rooted in its ability to discriminate between traffic, to decide what should be permitted, prioritized, and what should be 'cleaned'. An ISP that operates a smart pipe is acting as traffic police and as a gatekeeper. While the dumb pipe refers to the mythical past of the end-to-end internet, the smart pipe belongs to the future of the 'internet-of-things'. Smart pipes can unlock "a pot of gold at the end of the rainbow for many organizations" -- that is, as long as the "threat" of net neutrality does not get in the way (Macaulay, 2015).[318]

The idea of an ISP acting as a dumb pipe aligns with the end-to-end principle often cited to justify net neutrality (Wu, 2003, p. 146), as well as the pre-internet regulatory notion of the

[318] U.S. FCC Chairman Ajit Pai, speaking to the 2017 Canadian Telecom Summit on the harms of net neutrality regulation (specifically, common carrier principles), stated that "to realize the digital future, we need smart infrastructure, not dumb pipes" (Pai, 2017).

“mere conduit” (see Winseck, 2015a). In simplified terms, net neutrality advocates are opposed to ISPs discriminating among internet traffic. However, subjecting different packets to different treatment has long been common practice for ISPs (McTaggart, 2006), and is also seen as key to their future, with experts warning that the “internet of things” will be impossible without ISPs taking an active role managing internet traffic (Hecht, 2015; Macaulay, 2015).[319] As one telecom executive stated in 2012, “what scares all carriers about network neutrality-type rhetoric is that they may actually lose the ability to control how they manage their networks when it comes to public Internet traffic” (Parsons, 2013, p. 96).

Since the mid-2000s, net neutrality has been one of the most contentious internet policy issues around the world. In part, this is because a variety of nation-specific issues, such as CRTC contests over zero-rating (Dobby, 2015a; Meyer, 2015), or Canada's UBB debate (see Chapter 3), can be aligned with a broader discussion of net neutrality.[320] It is also because net neutrality issues cut to the heart of questions about what an intermediary should me. A lot of the positive potential of the internet can be attributed to its 'openness'; the end-to-end principle, dumb pipes, and decentralized governance allowed for the development of innovative uses (van Schewick, 2010). Hence, net neutrality and “open internet” are often synonymous (FCC, 2015), and groups like OpenMedia maintain openness as a key principle of their advocacy. In contrast, the smart

[319] The internet of things (IoT) refers to the proliferation of networked sensors and computers throughout our environment, which communicate with one another using internet protocols. As a former Security Liaison Officer at Bell recently argued about this transformation: "The novel thing here, the thing that changes from an IT architecture, is the gateway element. Gateways in IT are often dumb, they move packets back and forth, they do network address translation and not much more... In the IoT, these things become security-critical elements in the infrastructure. And this is because the devices at the edge of the network cannot be relied upon to protect themselves. So the last hop in the network, which is the gateway, takes on a lot of functionality" (Macaulay, 2015).

[320] Net neutrality is not defined as a regulatory concept in Canada. The regulatory regime relevant to net neutrality includes Internet Traffic Management Practices, or ITMPs (CRTC, 2009b; Parsons, 2013, Chapter 4), the CRTC's objective under the Telecommunications Act to prevent unjust discrimination or undue preference, and the regulatory framework for differential pricing (CRTC, 2015a, 2017).

pipe does not necessarily represent a closed internet, but it does allow for a controlled, hygienic internet, with ISPs acting as gatekeepers.

Net neutrality advocates sometimes warn that discrimination by ISPs will produce “walled gardens” (Crawford, 2013, pp. 158–160), hearkening back to the days of CompuServe and AOL, but the more appropriate metaphor for smart pipes is that of the semi-permeable membrane. Instead of walls, smart pipes have programmable gateways, protecting us from “dirty” (Reo, 2016) and malicious elements. All traffic in and out of the network is inspected and categorized. Some packets may pass, others are blocked or diverted. There are net neutrality advocates who accept the need for such systems to deal with malicious traffic and for other legitimate network management purposes (Hecht, 2015; van Schewick, 2010), but this shifts the question to ask which discriminations are legitimate. The most contentious forms of differential treatment do not involve security, but more direct ways of maximizing profit, such as vertically-integrated incumbents privileging their own content or providing certain content with a “fast lane” in exchange for payment (FCC, 2015). However, while the practice of intermediaries granting “undue preference” to certain traffic for commercial reasons has received critical attention and regulatory disapproval in Canada (CRTC, 2015a, 2017; Dobby, 2015a), the transformation to smart pipes has proceeded quietly in the interests of security.

State partners, security providers, and the struggle for standards

While the previous chapter addressed the discretion ISPs enjoy as privacy custodians, and how different organizations choose to pursue these responsibilities, this chapter dealt with efforts to promote the standardization of ISPs' security responsibilities as a way of limiting discretion.

For lawful access, standardization has been pursued through legislation that would mandate certain practices and surveillance equipment, while cyber security has thus far been addressed through voluntary standards and government-industry partnerships or superstructural nodes.

Lawful access and cyber security can be thought of as routine operational practices for ISPs, which have historically partnered and collaborated with state agencies, and cooperated within the industry in pursuit of a common approach. Canadian ISPs generally recognize security as part of their public obligations, whether this means assisting law enforcement or countering network attacks, and they perform a great deal of this work beyond their legal obligations. Unlike regulation-for-competition, in which a regulator structures market relationships that would not otherwise exist, intermediaries often govern security of their own accord in ways that complement the interests of state agencies.

But this has not been a harmonious realization of regulatory capitalism, since organizations exercise significant discretion in meeting their security responsibilities and conduct across the industry is far from uniform. Liberalization has also created market forces that sometimes contradict this public policy objective, when the costs of security become a competitive disadvantage. Finally, ISPs are forced to mediate when state and customer interests contradict each other, such as when police request customer information. As a result, security regulation has been an ongoing governmental priority since the start of the 2000s, leading to some new legal obligations for intermediaries and recurring attempts to legislate lawful access standards. However, Canadian regulators have shown a reluctance to impose standards for the dynamic and expanding set of techniques that govern cyber security, in favor of a more collaborative approach. Part of the reason for this reluctance is that governing cyber security means governing some of the fundamental ways through which the internet operates.

Efforts to standardize lawful access reflect the persistent need of state agencies to identify individuals through digital traces and to intercept communications, both of which depend on partnering with intermediaries whose infrastructure makes communications possible. While the basic surveillance responsibilities of lawful access are outgrowths of telephone-era requirements, cyber security represents a much broader, future-oriented kind of rationality, in which ISPs govern internet traffic in the interests of security. Underlying the shift to cyber security is a fundamental transformation in the role of the ISP as a governing institution – a transformation that has been underway since the early days of the internet's commercialization but which now signals a clear break from what is commonly given as the internet's founding ethos. This is the transformation away from the ideal of the end-to-end network, where ISPs merely act as conduits or dumb pipes, and toward the ISP as a smart pipe that surveils and discriminates between data packets. The adoption of this new role and its accompanying rationality has proceeded with little controversy by targeting universally-despised forms of traffic such as child pornography, spam, and denial-of-service attacks, thereby eliding the net neutrality concerns that arise when surveillance and discrimination are used for other purposes. ISPs have gone from assisting state security and policing agencies, to also policing traffic of their own accord and ensuring the security of the digital flows we all depend on. ISPs have become key security providers rather than simply the state’s partners in security. This transformation is indicative of the increasingly active role intermediaries now play in governing digital flows, the growing value of connectivity, and the corresponding increase in the harms caused by threats circulating through our digital networks.

Conclusion

This dissertation analyzed how intermediaries function as governing nodes, and are increasingly used as instruments of public policy in Canada. It contributes to our understanding of contemporary connectivity by foregrounding ISPs as instruments of internet governance and by drawing on theoretical perspectives largely missing from internet governance scholarship. Governmentality and nodal governance are valuable analytic resources that can help us understand the heterogeneous means through which power operates in our society and to attend to the details or specific techniques of governance. However, I argue that an empirical analysis along these lines must also include a conceptualization of agency and sovereignty, which are often underemphasized or missing in studies of governmentality.

First, contra popular interpretations of Foucault, our analyses should be populated by actors as well as technologies, discourses, and rationalities. We need to discuss agency as purposive decision-making and to extend collective agency to institutions. This means recognizing that both individuals and organizations make choices and do things, and this is crucial in making sense of the discretion that ISPs exercise when addressing many of their social and regulatory responsibilities, such as providing access to both the public and their competitors (Chapters 2 and 3), protecting user privacy (Chapter 4), and governing malicious traffic (Chapter 5). Discretion is "all-pervasive" and inevitable in the application of laws (Hawkins, 1992, p. 11), as actors interpret their constraints and work within them. Discretion varies in extent from one set of circumstances to the next, but there is always some flexibility for actors and this freedom is often highly desirable. ISP responsibilities include some that are informal, voluntary, and inconsistent (media literacy, equitable connectivity), while others may trigger legal liability (non-discrimination, privacy, lawful access). However, in all cases intermediaries are collective actors with decisions to make, and it is through these different decisions that ISPs distinguish themselves.

In addition to agency, we need to discuss the relationship between state and non-state actors, which means acknowledging sovereignty as a claim to territorial supremacy. This supports Mitchell Dean's (2007) call to "recover sovereignty" in political theory (including governmentality studies), seeking to displace the "seductive narrative" of a shift away from territorial states and towards networked governance (p. 14). Sovereignty is particularly relevant for internet governance if we include domestic actors like ISPs in our analysis (Zajko, 2016a), since ISPs operate material infrastructure that is rooted in territories and jurisdictions, and are closely regulated by multiple state agencies.

The work of Foucault, Latour, and nodal governance scholars has frequently been used to de-center the state in theories of governance, with power being the product of shifting networks and alliances that can be described without recourse to sovereignty. Nodal governance scholars (Johnston & Shearing, 2010; Wood & Shearing, 2007) encourage us not to grant state actors conceptual priority, and even Dean argues that sovereignty cannot simply be presumed, since "the existence of something that approximates a sovereign agent within a geographical space is open to empirical investigation" (2007, p. 141). However, none of this means that we should presume sovereignty is irrelevant, or that state-centric forms of governance do not exist. Nodal governance scholarship encourages us to consider the plurality of state and non-state agents involved in governance, and private companies and associations are clearly important in this regard. But this empirical investigation also shows how ISPs in Canada presume the existence of state actors that are supreme within their territories, and that state authorities are also the primary means of imposing new responsibilities on intermediaries. Rather than indicating a decline of state sovereignty, this is compatible with a shift where "state power is now even more diffuse and pervasive through the ways in which it governs through the knowledge, capacity and resources of others" (Wood & Shearing, 2007, p. 33).

This is not to say that state agencies simply impose their sovereign will on intermediaries – Chapter 2 covers cases where public agencies act primarily as sources of funding for intermediaries to pursue the public interest, and in Chapter 5 I described the state's coordinating role in cyber security's superstructural nodes – but in all chapters these state nodes play a distinct role, by championing issues outside the ambit of market actors and by setting the terms under which intermediaries operate. Even though the CRTC makes decisions following submissions from interested parties and has been criticised for serving the interests of incumbents, its rulings are sometimes deeply unpopular among these giant firms. Ultimately, incumbents have no choice but to recognize CRTC decisions as sovereign claims unless these are overruled by a higher power (Federal Court or federal Cabinet).

While sovereignty should not be a starting assumption when we encounter state actors in an empirical analysis, we need to acknowledge when we see it and to find ways to characterize relations between state and non-state actors. To this end, neoliberalism cannot be presumed as a backdrop for telecom liberalization, but refers instead to a specific rationality based around key principles (market forces, limited government) which can be proclaimed without being implemented. Instead of neoliberalism, regulatory capitalism provides a more useful description of an arrangement where market forces are expected to govern connectivity, but market forces themselves must be continuously governed by the state. In the rest of this conclusion I will discuss what this dissertation can tell us about intermediation under these conditions.

(Dis)intermediation

Around the world, ISPs are implicated in a growing range of social relationships. In Canada, this trend also reflects all of the ways that market forces alone cannot meet public policy objectives, like equitably distributing connectivity, protecting privacy, or public safety. Furthermore, under regulatory capitalism the rationality of regulation-for-competition is based on the idea that the market itself is a problem that needs to be governed, by imposing obligations on ISPs to relate to each other in certain ways.

As pure intermediaries, ISPs sit passively between the 'end points' of our online interactions. Their responsibility is to enable our relationships over their networks. Since we have permitted ISPs to be more than ‘mere conduits’ or ‘dumb pipes’, these institutions can also become actively involved in the flows passing through them. They inspect, discriminate, and police the connective fabric of society, either to meet requirements imposed by other actors or for their own reasons. Many of the social roles played by these intermediaries involve enacting distinct forms of rationality, such as the regulatory distinctions and justifications underpinning the mandated access regime, or the process of surveillance and classification that enables technical interventions against malicious traffic. Regardless of the specific role, all of these are instances of 'intermediation' – a process that installs new intermediaries in social roles, or expands the roles of existing intermediaries. This is important to consider, because the internet has often been described as a disintermediating force that cuts out intermediaries. Intermediation and disintermediation are actually both occurring simultaneously, but it is important to reflect on how these major social shifts relate to each other.

Part of the internet's foundational end-to-end principle discussed in the previous chapter was that 'endpoints' could connect by using a shared protocol, and intermediate networks simply pass these communications to their intended recipients (D. P. Reed, 2010; van Schewick, 2010). In this idealized model of the internet, ISPs effectively function as mere conduits, active only in making routing decisions. Connectivity removes the need for many kinds of pre-internet gatekeepers and go-betweens, like retailers, distributors, and publishers, and reduces the ability of traditionally dominant institutions to control information flows (DeNardis, 2014, p. 10). Hierarchies are flattened or collapsed, and for practical purposes, the result is an unmediated connection between the internet's 'endpoints' – a connection managed by ISPs.

If disintermediation is "the movement of power out of the middle of the net" (Moglen, 2012), then intermediation is a word we can use to describe the growing power of the 'middle'. If disintermediation means dismantling hierarchies and moving to peer relationships, intermediation is a process that installs new "feudal lords" (Schneier, 2012) and governs *through* these intermediaries (DeNardis, 2014). Where previously, each endpoint on the internet was reachable from any other, communications must now contend with intermediaries that may prove impassable. Relationships that used to be between two parties must now gain the consent of a third, and this third party is increasingly seen as a point of control where additional responsibilities can be applied.

Online intermediaries like Facebook are critically important, in large part because they sit atop vast quantities of personal data. But ultimately these are just services, and a world without

Facebook is not difficult to imagine. Many online intermediaries provide services that might conceivably be handled by endpoints rather than in the 'middle of the net', but the same cannot be said for the ISPs that act as internet's ultimate go-betweens (Kerr & Gilbert, 2004). ISPs cannot be disintermediated, since they provide the internet’s connective infrastructure (Goldsmith & Wu, 2006, pp. 70–73). The only meaningful alternatives to ISPs, like decentralized mesh networks, remain limited to localized contexts (LaFrance, 2014; Shaffer, 2011).

There is no question that, for the foreseeable future, ISPs will continue to occupy their central position. The important question is what kind of intermediaries these ISPs will be. The trend has been for ISPs to provide more services, to take on greater public policy responsibilities, and engage in more active interventions in traffic flows. These include inspecting and blocking malicious traffic, prioritizing some internet protocols over others, and implementing network address translation (NAT) that can 'break' end-to-end functionality.[321] The end-to-end ethos has not been entirely lost, as the aftermath of the Snowden revelations created increased demand for meaningful control over data and reduced dependence on third parties. But ISPs are the internet’s indispensable foundations. This is why we need to pay especially close attention to them, and the growing power of the nodes they operate.

As points of control over telecom infrastructure, ISPs are instruments of public policies to promote competitiveness in the telecom industry and connectivity throughout society. The responsibilities associated with these efforts have consequences for how ISPs govern us and our information, including our ability (or inability) to choose among ISPs with different policies. But another set of expectations and roles have been imposed on or adopted by ISPs specifically in relation to their control over internet traffic, content, and personal information (DeNardis, 2014,

[321] See note 13 above.

p. 11). These are a direct consequence of the growing importance of internet connectivity in society and the considerable power that ISPs can exercise as points of control. In this dissertation I have discussed ISPs as governing nodes in relation to privacy, copyright, security and net neutrality, but this list is by no means exhaustive and seems set to expand. This is why I have concluded with a discussion of cyber security, which has been used to justify a variety of new roles for intermediaries in different countries.

Another way to characterize intermediation is as an accumulation of social roles for intermediaries. Some of this is due to our growing expectations of these institutions, but many ISPs are also interested in expanding their services. As intermediaries take on a growing number of important roles in society, role conflicts accumulate and become more significant. Any attempt to provide connectivity as a public good runs against the expectations of liberalized telecom industry. Incumbents must simultaneously compete and cooperate with IISPs. Government agencies expect ISPs to act as partners in surveillance and security, but these expectations can conflict with the duties of privacy custodians. New kinds of traffic discrimination and manipulation challenge expectations of net neutrality.

ISPs exercise considerable discretion in addressing many of these conflicts, favoring some roles and expectations over others. Organizations that see ISPs as instruments of public policy have their own ways of resolving contradictory expectations, such as by forming partnerships with industry or mandating standardization. Some of the role conflicts listed above and their potential solutions have been among the most contentious public policy debates in recent Canadian history. Despite dramatic reversals on UBB and lawful access policy following public outcry, the fundamental conflicts at the heart of these issues remain and will resurface in new contests over what we expect from our intermediaries.

Addressing intermediation

In summary, the internet has covered society with a dense connective fabric. This allows for new kinds of relationships to be formed, some of which cut out previously-installed intermediaries. Disruption and 'creative destruction' became mantras as we did away with old and inefficient models in favor of decentralization and direct connections. But the connective fabric that covers the planet allows for new classes of intermediaries to manage our relationships – exchanging services for access to our data flows, providing security and convenience, and enforcing appropriate behavior. This trend extends to the ISPs that own and operate telecom infrastructure, and which now contend with a growing list of responsibilities.

The growing concentration of power in the middle of our networks can lead ISPs to exploit their nodal position, and reduces autonomy at the edges. An obvious solution to this is to stick to the internet's 'first principles' (Carpenter, 1996) – namely, end-to-end architecture. As net neutrality advocates argue, this would mean privileging endpoints, limiting intermediary functions, and enforcing constraints on intermediaries' discretion, so that control over a nodal position only confers limited power over data flows. There are good reasons to support such an argument, but this needs to be coupled with a recognition that users have long since traded the autonomy and bewilderment of the early internet for convenience and security (Schneier, 2012; Zittrain, 2008), and that ISPs have acted as more than conduits since the beginnings of the industry. Alongside the intermediation that led to new service offerings and middleman roles, ISPs became instruments in a range of public policies, promoting connectivity (Chapter 2), competition (Chapter 3), privacy and security (Chapters 4 & 5). Even in a simpler context, when an ISP was little more than an “on-ramp to the 'information highway'” (Hunt, 2014, p. 32), roadmaps for the future envisioned connectivity as a means of achieving political objectives such as cultural sovereignty (Industry Canada, 1994) and local autonomy (Telecommunities Canada & Industry Canada, 1997), and these visions themselves became an object of political struggle (M. Fraser, 1999, pp. 68–70; G. Graham, personal communication, September 26 & 27, 2015).

In short, there is no going back to a mythical time when ISPs were apolitical and confined to simply providing connectivity. This was a state of affairs that never truly existed, and many of the new roles that ISPs have adopted are a response to the dramatic changes the internet has undergone since commercialization and liberalization. Whether or not intermediation is desirable depends on the set of responsibilities we are considering, and there are difficult policy decisions with strong arguments both for and against intermediation when it comes to discriminating amongst illegal or malicious content (child pornography and cyber attacks), or the kinds of discrimination that some argue is vital for the “internet of things” to develop (see Chapter 5).

While we should not romanticize a past of unfettered connectivity that never existed, we can remember what made the internet so revolutionary: interactive connections between the endpoints, allowing for the removal or replacement of traditional intermediaries, and new kinds of social relationships. Preserving this transformative potential is particularly important as the internet's topography and architecture 'flattens' – a process of consolidation which I described in the Introduction. To address these stakes, we must take up the question of just how large and powerful we want the actors making these decisions to be.

Diversity, consolidation and concentration of power

Following liberalization, the trend in Canadian telecom has been towards consolidation, meaning that the giant firms which mediate our social relationships have grown bigger. While there is now less room for concentration in the Canadian telecom industry, the number of incumbents could be further reduced, and the survivors further enlarged, if regulators allowed. In addition, there are hundreds of Canadian ISPs that are protected from unbridled market power by the CRTC's regulatory regime. While IISPs are usually dependent on incumbent infrastructure and are frequently referred to as 'resellers' (of an incumbent's product), these smaller intermediaries take a variety of organizational forms and approaches to the problems of connectivity. Their existence is marginal in many ways, and the ability of new entrants to innovate in the market or grow into true competitors against the incumbents is severely limited. But the capacity to create and operate alternative kinds of intermediaries is an important aspect of the internet's foundational architecture.

While internet access is not a natural monopoly, this does not necessarily mean that connectivity is best provided through market competition. There is no technical reason why telecom networks of various kinds and sizes cannot coexist, overlap and interconnect. This is after all what the internet was designed to accomplish – allowing Autonomous Systems to communicate.[322] The internet's 'openness' to new and diverse entities is a fundamental characteristic, but this openness depends less on protocols and institutions devoted to internet governance (like ICANN and the IETF), and more on the ISPs that have ended up dominating in a geographic area.

The reasons why there is often limited diversity among ISPs in a given 'territory' include

[322] See note 8 above.

the concentrations of power that were inherited from the monopoly era (incumbency), the competitive rationality that conceives of ISPs as market actors (expected to exploit their differentials in power), and the material challenges of establishing a new network, which include access to property, infrastructure, and the electromagnetic spectrum. Under regulatory capitalism, all of these elements are subject to government regulation with the intent of controlling market power and promoting competition, but these regulations have been much more effective at the former than the latter. Still, even if the assumptions of regulation-for-competition have been mistaken and we cannot expect new competitors to challenge the incumbents, at the very least the regulatory regime maintains the possibility that other kinds of intermediaries can co-exist and benefit from protections such as mandated access. This allows us to imagine intermediaries exercising their discretion in novel ways, the question being, what kinds of intermediaries might these be, and how would they be different?

Alternative intermediaries

In addition to recognizing the diversity of governing actors or nodes in contemporary society, nodal governance scholarship often includes a strong normative orientation in preference of local, decentralized, and diverse forms of governance that enhance democracy and empower weak actors (Johnston & Shearing, 2003; Wood & Shearing, 2007). To translate these values to internet governance is not to say that all ISPs should be small and local, but at the very least it must be possible for such intermediaries exist. This is a possibility that can be denied when connectivity falls under centralized control, whether by a giant firm or the state, and it is important to ensure that new intermediaries can be created to address local needs and diverse values.

A persistent pattern in Canada's internet policy orientation since the mid-1990s has been the preservation of the status quo. This means legitimating the importance of dominant institutions, including incumbents and regulators, as well as using regulation to prevent or limit known problems, such as abuses of market power, or a final wave of consolidation that might clear the 'playing field' of many remaining ISPs. These tensions are described in Chapter 3, and leave the future open to three basic policy orientations.

The first option is to embrace the giant firm, and allow the incumbents to dominate as the inevitable consequence of the market. The second option is to preserve the status quo of regulatory capitalism, maintaining checks on incumbent dominance while protecting the existence of other intermediaries (IISPs) as a point of tension. This is the 'middle road' discussed in Chapter 3, and is the least controversial because it conserves existing power relations. The third option would involve promoting some alternative conception of intermediaries, or a new framework for how ISPs relate to one another.[323]

When considering alternate approaches, we would do well to look to the actors and rationalities covered in Chapter 2 that stand in contrast to incumbent-dominated liberalization. These include various ways of treating connectivity as a public good, or choosing something other than a market-based approach to the distribution of these networks. While even FreeNets must exchange money for services, this does not mean that commercial imperatives dominate. Alternative intermediaries are able to prioritize other values, such as inclusion, effective use and

[323] This might mean adopting a model based on structural separation (see Chapter 3), where ISPs are confined to a limited intermediary function, eliminating the possibility of media conglomerates taking advantage of their nodal position. Structural separation still aligns with a competitive rationality, where the benefits of connectivity are maximized through market competition, but competition occurs between services over a shared infrastructure rather than competing infrastructures.

local control. Some intermediaries continue to operate on the basis of these alternative rationalities within regulatory capitalism, in tension with its rationality of liberalization. But we should also remember a time that seemed less constrained, before the die was cast. The mid-1990s were a formative stage, and not a golden era of the internet. But this was also an imaginative period, in which various dreams of connectivity and cyberspace circulated and were sometimes implemented, as in the FreeNet movement. While many of these dreams are easily dismissed as 'cyber-utopian' (see Morozov, 2011), it does not follow that the existing political economy of telecom is natural, inevitable, or realist. Instead, we need to understand existing arrangements as the triumph of one rationality over others, which despite its dominance, has yet to foreclose other possibilities.

In this dissertation, I have examined intermediaries as instruments of public policy towards a variety of goals, and many of these objectives need not be uniformly or universally pursued. In other words, there is no one-size-fits-all answer to the problems of connectivity. The first public policy goal I analyzed, connectivity as an end in itself (Chapter 2), is the most fundamental, and echoes the universal service mandate of the telephony era. But this does not translate to monopoly control or a fibre connection for every home in the country, and how connectivity is promoted in an urban area should be quite different from a remote First Nation. Other goals covered in this dissertation, including competitive success, privacy, security, copyright, and net neutrality, are politically contingent, with active debates about what aspects should be left to the discretion of intermediaries.

Debates about standards and regulations are most important when subscribers lack meaningful choice between ISPs – a situation likely to continue under a regime of facilities-based competition. But as I argued in Chapter 2, the current regulatory regime is not the greatest obstacle to alternative intermediaries such as FreeNets, community networks, and ISPs that treat connectivity as a public good. Alternative intermediaries require support, and champions to mobilize this support. Institutions require organization and internal governance. Networks require infrastructure and capital, as well as accessible sources of upstream connectivity. Finally, the dominant rationality of liberalization (including facilities-based competition), in which connectivity is treated as a commodity best provided by private industry, is the chief obstacle to many projects that conceive of connectivity as some form of a public good.

To summarize, the process of intermediation is too complex to be generalized as desirable or harmful. There is little agreement about what intermediaries should be, or what values should shape their decisions, and we need not strive for such a consensus. Even local autonomy, a normative principle for both nodal governance scholars and community network advocates, is not a universal value in internet governance. Not every community wants to exercise local control over connectivity. And yet, the ability to do so should be preserved distinct from the end-to-end principle. If endpoints no longer have the sort of decision-making power they once did, if we have come to depend on intermediaries' discretion over many matters of increasing importance, then it must be possible for alternative intermediaries to exist, including those that serve a limited set of needs and values. This has nothing to do with reducing barriers to entry in order to promote a more competitive market, but is simply about allowing diverse and locally-specific forms of governance to address the problems of connectivity.

Looking to the Future

Canada has a rich history of governing communications for public ends, and intermediaries have been political instruments since some of the earliest days of telecommunications. I have documented these historical precedents for current debates, showing that in many cases, internet policy issues did not begin with the internet. What has changed is that connectivity is more vital for society than ever, and internet intermediaries now occupy an unprecedented number of social roles, engendering new possibilities for the future.

The scope of this analysis means that certain topics have remained largely unaddressed. By looking across Canadian institutions, the preceding chapters offer limited insight into international comparisons, and such comparative work could show the extent to which intermediaries' governing rationalities have propagated across borders or are unique to national contexts. In addition, we need more detailed accounts of what happens within institutions or governing nodes. How do organizations implement routine forms of governance? How do they undertake major decisions? How does individual agency and organizational structure shape collective agency? The answers to these questions will vary from one institution to the next, and the nodes discussed in this dissertation could yield particularly valuable lessons through detailed case studies. While it is safe to say that the CRTC will remain an important sovereign authority in Canada and incumbent ISPs will maintain their dominant economic position in the near future, studies of alternative intermediaries, such as community networks and local connectivity projects can also provide useful ideas for how to organize and govern connectivity. We need to better understand how these intermediaries can be established and structured, and useful strategies for keeping them attuned to the publics they serve.

Going forward, it is important to remember what makes the internet unique. Not just its pluripotency or ability to assume new forms, but its architecture and governance. It is amazing that this assemblage of highly diverse networks without central coordination works at all. This underlying fact may become less remarkable as it becomes less true, if the trend continues towards a 'flatter' internet topography involving fewer, larger intermediaries. But the lessons of the internet – the dual movement of disintermediation and intermediation, the use of robust protocols to interconnect diverse endpoints – can be learned again as required. For now, there is one set of institutions that cannot be disintermediated, which is why ISPs have been central to my analysis. For this reason, the struggles over ISPs as governing actors and points of control will continue to be crucial in a milieu where digitally-networked screens have become our primary means of relating to society.

References

AAMDC. (2011). *Connecting the Dots: Alberta Rural Broadband Coverage Study*. Retrieved November 27, 2017, from https://web.archive.org/web/20130424042018/http://www.aamdc.com/events-programs/convention-highlights/doc_download/983-2012-connecting-the-dots

Abbate, J. (1999). *Inventing the Internet*. Cambridge, MA: MIT Press.

Abma, D. (2014, April 28). “Mobile TV is a broadcasting service”: Bell. Retrieved April 29, 2014, from http://www.thewirereport.ca/news/2014/04/28/carriers-split-on-mobile-tv-definition/28197

Adams, R. (2014). Coquitlam Optical Network Corporation (QNet) 2013 Annual Report. Retrieved August 24, 2015, from http://www.qnetbc.net/docs/default-source/qnet-files/annual-reports/qnet_2013_annual_report.pdf

Adams, R. (2015, June 8). Bell Deferral Accounts & Eastern Ontarion Wardens Caucus (EORN). *DSL Reports*. Retrieved January 11, 2017, from http://www.dslreports.com/forum/r30100750-Bell-Deferral-Accounts-Eastern-Ontarion-Wardens-Caucus-EORN

Adams, R., & Coert, R. (2014). CRTC 2013-551 8663-C12-201313601 Review of Wholesale Services. Retrieved November 4, 2014, from https://services.crtc.gc.ca/pub/DocWebBroker/OpenDocument.aspx?DMID=2068368

Agriculture and Rural Development. (2009). *Rural Communities in Alberta and Broadband: Enabling a Culture of Use*. Retrieved November 27, 2017, from https://web.archive.org/web/20140327052019/http://www1.agric.gov.ab.ca/$department/deptdocs.nsf/all/csi12675/$FILE/rural_communities_and_broadband.pdf

Alberta Agriculture and Rural Development. (2014, October 2). Rural Connections: Community Broadband Infrastructure Pilot Program Approved Projects. Retrieved November 27, 2017, from https://web.archive.org/web/20160326075113/http://www1.agric.gov.ab.ca/$Department/deptdocs.nsf/all/csi12826

Alberta Economic Development Authority. (2010). *Accelerating Broadband Enablement in Rural Alberta*. Alberta Economic Development Authority. Retrieved October 22, 2013, from https://aeda.alberta.ca/media/6409/accelerating_broadband_rural_alberta.pdf

Alberta Venture. (2007, June 1). Most Respected Corporate Leaders: Art Price. Retrieved January 19, 2015, from http://albertaventure.com/2007/06/most-respected-corporate-leaders-art-price/

Anderson, S. (2011, March 28). The Great Internet Billing Debate: Stop the meter. Retrieved April 10, 2016, from http://business.financialpost.com/fp-comment/the-great-internet-billing-debate-stop-the-meter

Antoniadis, P., & Apostol, I. (2014). The Right(s) to the Hybrid City and the Role of DIY Networking. *The Journal of Community Informatics*, *10*(3). Retrieved from http://ci-journal.net/index.php/ciej/article/view/1092

Archer, M. S. (2000). *Being Human : The Problem of Agency*. Cambridge, U.K.: Cambridge University Press.

Arellano, N. (2011, June 27). Small ISPs foresee cost burden in ‘Lawful Access’ bills. Retrieved October 27, 2015, from http://www.itbusiness.ca/news/small-isps-foresee-cost-burden-in-lawful-access-bills/16419

Armstrong, C., & Nelles, H. V. (1986). *Monopoly’s Moment: The Organization and Regulation of Canadian Utilities, 1830-1930*. Philadelphia: Temple University Press.

At home with the NBN. (2011). Retrieved February 20, 2015, from https://www.youtube.com/watch?v=KgudKBZ-4HI&feature=youtube_gdata_player

Atria Networks. (2008, February 25). Hydro Ottawa to sell Telecom Ottawa to Atria Networks for $63 Million. Retrieved November 27, 2017, from https://web.archive.org/web/20101219063753/http://www.atrianetworks.com:80/news/hydro-ottawa-to-sell-telecom-ottawa-to-atria-networks-for-63-million/

Avis, A. W. (1995). *Public spaces on the information highway: The role of community networks* (M.A.). University of Calgary, Calgary.

Axia. (2011, September 20). Axia NetMedia Corporation Management’s Discussion & Analysis for the year ended June 30, 2011. Retrieved November 27, 2017, from https://web.archive.org/web/20150509182453/http://ir.axia.com/files/doc_financials/2011/MDA%20YE%20FY11%202011-9-20%20FINAL.pdf

Axia. (2013, March 14). Axia NetMedia Corporation Management’s Discussion & Analysis for the year ended December 31, 2012. Retrieved December 3, 2013, from http://ir.axia.com/files/doc_financials/2012/Dec2012MD&AFS_v001_l8d146.pdf

Axia. (2015, March 5). Axia NetMedia Corporation Management’s Discussion & Analysis for the year ended December 31, 2014. Retrieved November 27, 2017, from https://web.archive.org/web/20150319040804/http://ir.axia.com:80/files/doc_financials/2014/AXX-Q4-2014-MDAFS.pdf

Axia. (2017, January 10). Axia Announces Fibre Optic Expansion to Fairview, Alberta. Retrieved June 13, 2017, from https://blog.axia.com/blog/axia-announces-fibre-optic-expansion-fairview-alberta

Axia Supernet Ltd. v. Bell West Inc., ABQB 195 (Court of Queen’s Bench of Alberta February 26, 2003). Retrieved November 27, 2017, from http://www.albertacourts.ab.ca/jdb_new/public/qb/1998-2003/qb/Civil/2003/2003abqb0195.pdf

Babe, R. E. (1975). *Cable television and telecommunications in Canada: An economic analysis*. East Lansing: Division of Research, Graduate School of Business Administration, Michigan State University.

Babe, R. E. (1990). *Telecommunications in Canada*. Toronto: University of Toronto Press.

Babe, R. E. (2011). Control of Telephones: The Canadian Experience. In E. A. Comor (Ed.), *Media, Structures, and Power: The Robert E. Babe Collection* (pp. 119–133). Toronto: University of Toronto Press.

Bailey, S. (2007, February 7). `Up to our knees in evil’: police fight growing demand for web child porn. *Canadian Press*.

Barnard-Wills, D., & Ashenden, D. (2012). Securing Virtual Space Cyber War, Cyber Terror, and Risk. *Space and*

Culture, *15*(2), 110–123.

Barnes, A. (1986, May 2). CRTC ends monopoly on private-line phone service. *Globe and Mail*, p. B6.

Barnett, M. (1993). Institutions, Roles, and Disorder: The Case of the Arab States System. *International Studies Quarterly*, *37*(3), 271–296.

Bartleman, M. (2017, September 26). OI consolidation loan stalled. Retrieved November 27, 2017, from http://www.oldsalbertan.ca/article/OI-consolidation-loan-stalled-20170926

BCCLA. (2012, January 13). Moving Towards a Surveillance Society: Proposals to Expand "Lawful Access" in Canada. Retrieved November 27, 2017, from http://www.bccla.org/wp-content/uploads/2012/03/2012-BCCLA-REPORT-Moving-toward-a-surveillance-society.pdf

Beaudry, P. (2010). Wireline deregulation: The Canadian experience. *Telecommunications Policy*, *34*(10), 606–615.

Bell. (2004, March 11). Written Representations. Retrieved November 27, 2017, from https://cippic.ca/sites/default/files/file-sharing-lawsuits/Bell_Written_Submissions.pdf

Bell. (2015, October 20). Petition to the Governor in Council to Vary Telecom Regulatory Policy CRTC 2015- 326, Review of wholesale wireline services and associated policies. Retrieved November 27, 2017, from https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/TRP-CRTC-2015-326-Bell-Canada-Petition-EN.pdf/$FILE/TRP-CRTC-2015-326-Bell-Canada-Petition-EN.pdf

Bell, Rogers, & TELUS. (2013a). Fair For Canada. Retrieved December 2, 2015, from https://web.archive.org/web/20131112000745/http://fairforcanada.ca/

Bell, Rogers, & TELUS. (2013b, July 9). Letter to the Prime Minister. Retrieved December 2, 2015, from https://web.archive.org/web/20130805230659/http://fairforcanada.ca/letter-to-prime-minister.pdf

Bendrath, R. (2007). The Return of the State in Cyberspace: The Hybrid Regulation of Global Data Protection. In M. Dunn, S. F. Krishna-Hensel, & V. Mauer (Eds.), *The Resurgence of the State: Trends and Processes in Cyberspace Governance, Aldershot: Ashgate* (pp. 111–151).

Bendrath, R., & Mueller, M. (2011). The End of the Net as We Know It? Deep Packet Inspection and Internet Governance. *New Media & Society*, *13*(7), 1142–1160.

Bernal-Castillero, M. (2013, October 1). Canada's Federal Privacy Laws (Background Paper No. 2007-44-E). Library of Parliament. Retrieved November 27, 2017, from http://www.parl.gc.ca/Content/LOP/ResearchPublications/2007-44-e.htm

Bevir, M. (1999). Foucault and Critique: Deploying Agency against Autonomy. *Political Theory*, *27*(1), 65–84.

Biddle, B. J. (1986). Recent Development in Role Theory. *Annual Review of Sociology*, *12*, 67–92.

Birdsall, W. F. (2000). The Digital Divide in the Liberal State: a Canadian Perspective. *First Monday*, *5*(12). Retrieved November 27, 2017, from http://firstmonday.org/ojs/index.php/fm/article/view/820/729

Birnhack, M. D., & Elkin-Koren, N. (2003). The Invisible Handshake: The Reemergence of the State in the Digital Environment. *Virginia Journal of Law and Technology*, *8*(2), 1–57.

Blackburn, S. (2013, August 7). Proud of our commitment to privacy in Canada. Retrieved February 4, 2016, from http://blog.telus.com/public-policy/proud-of-our-commitment-to-privacy-in-canada/

Blais, J.-P. (2016, November 16). Getting ahead of the curve - Jean-Pierre Blais to the Canadian Chapter of the International Institute of Communications [Speeches]. Retrieved November 17, 2016, from http://news.gc.ca/web/article-en.do?nid=1154239

BMG Canada Inc. v. John Doe (2004), 3 FCR 241. Retrieved December 4, 2017, from https://www.canlii.org/en/ca/fct/doc/2004/2004fc488/2004fc488.html

Bodnar, C. (2007). The Vancouver Community Network, Social Investing and Public Good Models of ICT development. *The Journal of Community Informatics*, *3*(4). Retrieved November 27, 2017, from http://ci-journal.net/index.php/ciej/article/view/307

Bogner, A., Littig, B., & Menz, W. (Eds.). (2009). *Interviewing Experts*. New York: Palgrave Macmillan.

Bostelaar, R. (2009, December 31). Robust Datapac finally retires; For three decades the Nortel-developed network kept the money flowing. Robert Bostelaar reports. *The Ottawa Citizen*.

Boutilier, A. (2015a, April 16). Bell Canada is facing a $750 million class action lawsuit over a program that tracked its users' internet usage to sell advertising. *The Toronto Star*. Retrieved from http://www.thestar.com/news/canada/2015/04/16/bell-faces-750m-lawsuit-over-advertising-program.html

Boutilier, A. (2015b, July 12). Internal RCMP documents show no significant problems with court decision requiring police to get a warrant to obtain telecom customers' data. *The Toronto Star*. Retrieved November 27, 2017, from http://www.thestar.com/news/canada/2015/07/12/halt-to-warrantless-disclosures-not-hindering-rcmp-say-documents.html

Boutilier, A., & McLeod, P. (2014, September 17). Police continue to request Canadians personal information from telecoms. Sometimes with a warrant, sometimes without a warrant. *The Toronto Star*. Retrieved November 27, 2017, from http://www.thestar.com/news/canada/2014/09/17/supreme_court_ruling_hasnt_stopped_police_from_warrantless_requests_for_data.html

Bower, D. (2012, February). *Promoting Next Generation Broadband Infrastructure in Ontario*. Retrieved June 3, 2013, from http://www.amo.on.ca/wcm/Documents/amo/Economic%20Development/MEDIPromotingNextGenerationBroadbandInfrastructureinOntario.pdf

Bowker, G. C., & Star, S. L. (1999). *Sorting things out: classification and its consequences*. Cambridge, MA: MIT Press.

Braga, M. (2016, December 20). Canadian telecoms push back on proposed police powers. Retrieved December 20, 2016, from http://www.cbc.ca/news/technology/rogers-teksavvy-itac-cwta-bill-c51-national-security-1.3903930

Braithwaite, J. (2004). Methods of power for development: weapons of the weak, weapons of the strong. *Michigan Journal of International Law*, *26*, 297–330.

Braithwaite, J. (2008). *Regulatory Capitalism: How It Works, Ideas for Making It Work Better*. Cheltenham: Edward Elgar.

Braithwaite, J., & Drahos, P. (2000). *Global Business Regulation*. Cambridge, U.K.: Cambridge University Press.

Brodkin, J. (2015, February 16). AT&T charges $29 more for gigabit fiber that doesn't watch your Web browsing. Retrieved February 9, 2016, from http://arstechnica.com/business/2015/02/att-charges-29-more-for-gigabit-fiber-that-doesnt-watch-your-web-browsing/

Bronskill, J. (2014, December 1). Feds were worried as telecom firm planned to go public on police access to Canadians' phone calls and emails, memo shows. Retrieved January 15, 2016, from http://news.nationalpost.com/news/canada/feds-were-worried-as-telecom-firms-planned-to-go-public-on-police-access-to-canadians-phone-calls-and-emails-memo-shows

Bronskill, J. (2015a, January 12). Police forces balk at tracking fees imposed by Rogers. Retrieved January 12, 2015, from http://www.cbc.ca/1.2897540

Bronskill, J. (2015b, August 24). Feds ponder warrantless police access to Internet subscriber info: chiefs. Retrieved August 24, 2015, from http://www.nationalnewswatch.com/2015/08/24/feds-ponder-warrantless-police-access-to-internet-subscriber-info-chiefs/

Brown, J. (2009, November 10). How Bell Canada is keeping tabs on telecom fraud. Retrieved November 27, 2017, from http://www.canadiansecuritymag.com/Risk-Management/News/How-Bell-Canada-is-keeping-tabs-on-telecom-fraud/Page-1.html#topart

Brown, W. (2015). *Undoing the Demos: Neoliberalism's Stealth Revolution*. New York: Zone Books.

Bull, S. (2017, March). *Addressing the Myths: SuperNet & Rural Broadband Internet*. Retrieved November 27, 2017, from http://www.vanhorneinstitute.com/wp-content/uploads/2017/04/Stephen-Bull-2017_03_16_SuperNet_DigitalFutures_Final.pdf

Burris, S., Drahos, P., & Shearing, C. (2005). Nodal governance. *Australian Journal of Legal Philosophy*, *30*, 30–58.

Burns, J. (1969, June 27). 58 wiretaps last year, Mackey says. *Globe and Mail*, pp. 1–2.

Cabinet Office. (2011). Cyber Security Strategy. Retrieved November 27, 2017, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

CACP. (2012). Simplifying Lawful Access – Bill C-30 – Through the Lens of Law Enforcement. Retrieved November 22, 2015, from https://web.archive.org/web/20120527181033/http://www.cacp.ca/media/library/download/1243/Final_Simplifying_Lawful_Access_final_english.pdf

Calabrese, L. (2013, June 12). The death of the community based network and the naughty people who killed it. Retrieved November 27, 2017, from http://frontiernetworks.ca/the-death-of-the-community-based-network-and-the-naughty-people-who-killed-it/

Caldwell, R. (2007). Agency and Change: Re-evaluating Foucault's Legacy. *Organization*, *14*(6), 769–791.

Calgary Regional Partnership. (2015, June 17). Notes from CRP Broadband Information Session. Retrieved January 17, 2017, from http://calgaryregion.ca/dam/Website/reports/members_docs/economic_prosperity/2015-Economic-Prosperity-Committee/September-2015/Notes-from-Calgary-Region-Broadband-Workshopheld-in-Okotoks--June-17--2015/Notes%20from%20Calgary%20Region%20Broadband%20Workshop%20held%20in%20Okotoks,%20June%2017,%202015.pdf

Canadian Committee on Corrections. (1969). *Recommendations of the Canadian Committee on Corrections [Ouimet report]*. Ottawa: The Queen's Printer. Retrieved November 27, 2017, from https://web.archive.org/web/20160214103543/http://www.johnhoward.ca/media/(1969)%20HV%208395%20A6%20C33%201969%20(Ouimet).pdf

Canadian Independent Telephone Association. (1911). Sixth Annual Convention - Official Report. *Canadian Municipal Journal*, *7*(12), 484–487.

Canadian Press. (1996, February 29). BC Tel, cable move closer to Internet battle (with introduction of Sympatico by phone company). *Canadian Press*.

Canadian Press. (2012, February 17). Online Snooping Bill Creates "Inspectors" With Unfettered Access To Internet Records: Report. Retrieved December 5, 2015, from http://www.huffingtonpost.ca/2012/02/17/lawful-access-telecoms_n_1284120.html

CANARIE. (n.d.). Cloud Technology: DAIR. Retrieved January 16, 2015, from http://www.canarie.ca/cloud/

CA*net Institute. (2001). A nation goes online: Canada's Internet history. Retrieved November 27, 2017, from http://www.canarie.ca/?mdocs-file=3407&mdocs-url=3406

Carpenter, B. E. (Ed.). (1996). RFC 1958: Architectural Principles of the Internet. Retrieved November 27, 2017, from https://tools.ietf.org/html/rfc1958

Carpenter, B. E., & Brim, S. W. (2002). *Middleboxes: Taxonomy and Issues* (RFC 3234). Retrieved November 27, 2017, from https://tools.ietf.org/html/rfc3234

Cashman, T. (1972). *Singing Wires: the Telephone in Alberta*. Edmonton: Alberta Government Telephone.

Castells, M. (2009). *Communication power*. Oxford: Oxford University Press.

Castlegar News. (2014, January 23). Broadband in the Columbia Basin. Retrieved November 27, 2017, from http://www.castlegarnews.com/news/241745161.html

Cave, M. (2006). Encouraging infrastructure competition via the ladder of investment. *Telecommunications Policy*, *30*(3), 223–237.

Cavoukian, A. (2011, December 6). Lawful access. *The Globe and Mail*, p. A.14.

CBC News. (2007, September 12). Government moving to access personal info, sparking privacy fears. Retrieved October 26, 2015, from http://www.cbc.ca/news/technology/government-moving-to-access-personal-info-sparking-privacy-fears-1.631075

CBC News. (2009, June 18). ISPs must help police snoop on internet under new bill. Retrieved December 5, 2015, from http://www.cbc.ca/news/technology/isps-must-help-police-snoop-on-internet-under-new-bill-1.817756

CBC News. (2013, August 31). Some TekSavvy internet customers upset by long service outages. Retrieved November 27, 2017, from http://www.cbc.ca/1.1309647

CCAICE. (2005, May 11). Canadian Coalition Against Internet Child Exploitation Releases National Action Plan. Retrieved November 27, 2017, from https://www.cybertip.ca/app/en/media_release_ccaice_action_plan

CCAICE. (n.d.). Retrieved November 19, 2015, from https://www.cybertip.ca/app/en/projects-ccaice

CCIRC. (2016). Cyber Security Technical Advice and Guidance. Retrieved August 15, 2016, from http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tchncl-dvc-gdnc-eng.aspx

Chander, A. (2013). How Law Made Silicon Valley. *Emory Law Journal*, *63*, 639.

Chase, S., & Marlow, I. (2011, February 1). Harper steps into Web dispute. Retrieved April 10, 2016, from http://www.theglobeandmail.com/technology/tech-news/harper-steps-into-web-dispute/article565219/

Chen, B. X. (2014, November 4). Verizon Wireless Under Fire for Ad-Targeting Program. Retrieved February 9, 2016, from http://bits.blogs.nytimes.com/2014/11/04/verizon-wireless-under-fire-for-ad-targeting-program/

Cherry, B. A. (2015). Technology transitions within telecommunications networks: Lessons from U.S. vs. Canadian policy experimentation under federalism. *Telecommunications Policy*, *39*(6), 463–485.

Chorney, N. M. (1964). Wiretapping and Electronic Eavesdropping. *Criminal Law Quarterly*, *7*, 434.

Chung, E. (2013, July 19). Small Alberta town gets massive 1,000 Mbps broadband boost. Retrieved November 27, 2017, from http://www.cbc.ca/news/technology/story/2013/07/17/technology-gigabit-internet-olds.html

CIRA. (2014, September 3). New system sends life-saving text messages to residents of Vancouver's Downtown Eastside. Retrieved November 27, 2017, from https://web.archive.org/web/20150907194255/http://cira.ca/news/new-system-sends-life-saving-text-messages-residents-vancouvers-downtown-eastside

City of Calgary. (2014a, November). *Presentation to the Canadian Radio-television and Telecommunications Commission*. Retrieved November 27, 2017, from https://services.crtc.gc.ca/pub/ListeInterventionList/Documents.aspx?ID=212360&Lang=e

City of Calgary. (2014b, December 19). Final Submissions of the City of Calgary. Retrieved from November 27, 2017, https://services.crtc.gc.ca/pub/ListeInterventionList/Documents.aspx?ID=212360&Lang=e

City of Kamloops. (2015). Kamloops Community Network. Retrieved July 25, 2015, from http://www.kamloops.ca/it/kcn.shtml

City of Kelowna. (2015). Quarterly Report: January to March 2015. Retrieved July 25, 2015, from http://www.kelowna.ca/CityPage/Docs/PDFs/%5CCommunications/2015-Q1_report.pdf?t=035527771

City of Nelson. (n.d.). Nelson Broadband Fibre Network. Retrieved July 25, 2015, from http://nelsonbroadband.com/broadband-service/

City of Ottawa. (2003). Ottawa 20/20 Broadband Plan - Final Draft. Retrieved July 22, 2015, from https://web.archive.org/web/20040415154114/http://www.ottawa.ca/2020/bb/pdf/bb.pdf

City of Penticton. (2014). Official Community Plan Bylaw No. 2002-20. Retrieved August 23, 2015, from http://www.penticton.ca/assets/City~Hall/Bylaws/Land~Use/Bylaw%202002-20-OCP-%20current%20to%20March%202014.pdf

Claridge, T. (1972, March 18). Application for order to chief: Ruling reserved on challenge of police wiretaps.

Globe and Mail, p. 61.

Clement, A., & Obar, J. (2015, March 12). Keeping Internet Users in the Know or in the Dark: Data Privacy Transparency of Canadian Internet Carriers - 2014 Report. Retrieved March 17, 2015, from https://openmedia.ca/sites/openmedia.ca/files/Keeping%20Internet%20Users%20in%20the%20Know%20or%20in%20the%20Dark%20-%202014%20March%2012%20FINAL.pdf

Clement, A., & Shade, L. R. (2000). The Access Rainbow: Conceptualizing universal access to the information/communications infrastructure. In M. Gurstein (Ed.), *Community informatics: Enabling communities with information and communications technologies* (pp. 32–51). Hershey: Idea Group.

CNOC. (2013, September 27). Part 1 application requesting relief to improve the quality of wholesale high-speed access services provided by cable carriers. Retrieved November 27, 2017, from https://services.crtc.gc.ca/pub/TransferToWeb/2013/8660-C182-201313113.zip

CNOC. (2014, October 24). Reply of Canadian Network Operators Consortium Inc. Retrieved November 27, 2017, from https://services.crtc.gc.ca/pub/ListeInterventionList/Documents.aspx?ID=212341&Lang=e

Cohen, J. E. (2012). *Configuring the Networked Self*. New Haven, CT: Yale University Press.

Cohen, S. A. (1982). Invasion of privacy: Police and electronic surveillance in Canada. *McGill Law Journal*, *27*, 619–675.

Collie, D. (2015, November 10). O-NET could become a nationwide Internet, phone, TV service provider. Retrieved January 30, 2017, from http://www.mountainviewgazette.ca/article/ONET-could-become-nationwide-20151110

Collison, M. (2003, Fall). Alberta SuperNet Connects: Big Sky Broadband. *Summit*. Retrieved November 27, 2017, from http://www.summitconnects.com/Articles_Columns/PDF_Documents/200310_01.pdf

Conference of Commissioners on Uniformity of Legislation. (1948). *Proceedings*.

Connecting British Columbia Agreement (2011). Retrieved from November 27, 2017, http://www.cio.gov.bc.ca/local/cio/strategic_partnerships/cbca.pdf

Cornfield, D. A. (1967). The Right to Privacy in Canada. *Faculty of Law Review (University of Toronto)*, *25*, 103–120.

Cox, J. (2012, December 18). Canada and the Five Eyes Intelligence Community. Retrieved November 27, 2017, from https://www.opencanada.org/features/canada-and-the-five-eyes-intelligence-community/

CPAC. (2010). *2010 Canadian Telecom Summit - Regulatory Blockbuster*. Retrieved November 27, 2017, from http://www.cpac.ca/en/programs/public-record/episodes/16021459

CPAC. (2011). *2011 Canadian Telecom Summit - Regulatory Blockbuster*. Retrieved November 27, 2017, from http://www.cpac.ca/en/programs/public-record/episodes/17096168

CPAC. (2012). *2012 Canadian Telecom Summit - Regulatory Blockbuster*. Retrieved November 27, 2017, from http://www.cpac.ca/en/programs/public-record/episodes/18503327

CPAC. (2013a). *2013 Canadian Telecom Summit - The Regulatory Blockbuster*. Retrieved November 27, 2017, from http://www.cpac.ca/en/programs/public-record/episodes/24774817

CPAC. (2013b). *IIC Conference: Consumer Policy Meets Consumer Populism*. Retrieved November 27, 2017, from http://www.cpac.ca/en/programs/public-record/episodes/28823095

CPAC. (2014). *2014 Canadian Telecom Summit - The Regulatory Blockbuster*. Retrieved November 27, 2017, from http://www.cpac.ca/en/programs/public-record/episodes/33776089

CPAC. (2015). *2015 Canadian Telecom Summit - The Regulatory Blockbuster*. Retrieved November 27, 2017, from http://www.cpac.ca/en/programs/public-record/episodes/39922612

Crang, M., Crosbie, T., & Graham, S. (2006). Variable Geometries of Connection: Urban Digital Divides and the Uses of Information Technology. *Urban Studies*, *43*(13), 2551–2570.

Crawford, S. (2013). *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age*. New Haven, CT: Yale University Press.

Cribb, R., & Greenblatt, M. (2015, November 5). Advanced encryption and search-warrant requirements have allowed child molesters, drug dealers and organized crime to hide their crimes from police. *The Toronto Star*. Retrieved November 27, 2017, from http://www.thestar.com/news/world/2015/11/05/advanced-encryption-privacy-measures-hinder-police-in-digital-age.html

Crouch, C. (2011). *The Strange Non-death of Neo-liberalism*. Cambridge, U.K.: Polity Press.

CRTC. (1985, August 29). Telecom Decision CRTC 85-19. Retrieved September 19, 2015, from http://www.crtc.gc.ca/eng/archive/1985/DT85-19.htm#archived

CRTC. (1992, June 12). Telecom Decision CRTC 92-12. Retrieved September 19, 2015, from http://www.crtc.gc.ca/eng/archive/1992/dt92-12.htm

CRTC. (1994, September 16). Telecom Decision CRTC 94-19. Retrieved August 11, 2015, from http://www.crtc.gc.ca/eng/archive/1994/dt94-19.htm

CRTC. (1995). *Competition and culture on Canada's information highway: Managing the realities of transition*. Ottawa: Canadian Radio-Television and Telecommunication Commission.

CRTC. (1997, May 1). Telecom Decision CRTC 97-8. Retrieved November 27, 2017, from http://www.crtc.gc.ca/eng/archive/1997/dt97-8.htm

CRTC. (1999, September 14). Telecom Decision CRTC 99-11. Retrieved March 4, 2016, from http://www.crtc.gc.ca/eng/archive/1999/DT99-11.HTM

CRTC. (2001). Order 2001-184. Retrieved March 3, 2016, from http://www.crtc.gc.ca/eng/archive/2001/O2001-184.htm

CRTC. (2002, May 30). Telecom Decision 2002-34. Retrieved November 27, 2017, from http://www.crtc.gc.ca/eng/archive/2002/dt2002-34.htm

CRTC. (2003a, May 30). Telecom Decision 2003-33. Retrieved October 2, 2013, from http://www.crtc.gc.ca/eng/archive/2003/dt2003-33.htm

CRTC. (2003b, July 11). Telecom Decision 2003-33-1. Retrieved October 2, 2013, from http://www.crtc.gc.ca/eng/archive/2003/dt2003-33-1.htm

CRTC. (2005, March 31). Telecom Decision CRTC 2005-20. Retrieved August 4, 2015, from http://www.crtc.gc.ca/eng/archive/2005/dt2005-20.htm

CRTC. (2006, March 29). Telecom Decision CRTC 2006-14. Retrieved August 4, 2015, from http://www.crtc.gc.ca/eng/archive/2006/dt2006-14.htm

CRTC. (2008, March 3). Telecom Decision CRTC 2008-17. Retrieved November 21, 2013, from http://crtc.gc.ca/eng/archive/2008/dt2008-17.htm

CRTC. (2009a, June 4). Telecom Decision 2009-326. Retrieved May 9, 2015, from http://www.crtc.gc.ca/eng/archive/2009/2009-326.htm

CRTC. (2009b, October 21). Telecom Regulatory Policy CRTC 2009-657. Retrieved August 23, 2016, from http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm

CRTC. (2009c, November 25). Telecom Regulatory Policy 2009-723. Retrieved November 22, 2015, from http://www.crtc.gc.ca/eng/archive/2009/2009-723.htm

CRTC. (2010a, August 30). Telecom Regulatory Policy CRTC 2010-632. Retrieved November 30, 2013, from http://www.crtc.gc.ca/eng/archive/2010/2010-632.htm

CRTC. (2010b, August 31). Telecom Decision 2010-639. Retrieved April 24, 2015, from http://www.crtc.gc.ca/eng/archive/2010/2010-639.htm

CRTC. (2010c, October 28). Transcript, Hearing 28 October 2010. Retrieved August 2, 2015, from http://www.crtc.gc.ca/eng/transcripts/2010/tt1028.html

CRTC. (2011a, January 13). Telecom Decision 2011-28. Retrieved April 24, 2015, from http://www.crtc.gc.ca/eng/archive/2011/2011-28.htm

CRTC. (2011b, January 25). Telecom Decision CRTC 2011-44. Retrieved April 13, 2016, from http://www.crtc.gc.ca/eng/archive/2011/2011-44.htm

CRTC. (2011c, July 18). Transcript, Hearing 11 July 2011, Review of billing practices for wholesale residential high speed access services. Retrieved November 19, 2013, from http://www.crtc.gc.ca/eng/transcripts/2011/tt0718.html

CRTC. (2011d, August 19). Broadcasting and Telecom Regulatory Policy CRTC 2011-512. Retrieved January 28, 2017, from http://www.crtc.gc.ca/eng/archive/2011/2011-512.htm

CRTC. (2011e, December 16). Telecom Order CRTC 2011-786. Retrieved April 13, 2016, from http://www.crtc.gc.ca/eng/archive/2011/2011-786.htm

CRTC. (2013a, February 21). Telecom Decision 2013-73. Retrieved May 4, 2016, from http://www.crtc.gc.ca/eng/archive/2013/2013-73.htm

CRTC. (2013b, June 20). Transcript, Hearing 20 June 2013. Retrieved August 4, 2015, from http://www.crtc.gc.ca/eng/transcripts/2013/tt0620.html

CRTC. (2013c, October 15). Telecom Notice of Consultation CRTC 2013-551. Retrieved November 4, 2014, from http://www.crtc.gc.ca/eng/archive/2013/2013-551.htm

CRTC. (2014a, July 31). Telecom Decision CRTC 2014-398. Retrieved May 8, 2016, from http://www.crtc.gc.ca/eng/archive/2014/2014-398.htm

CRTC. (2014b, October 1). Transcript, Hearing October 1, 2014, Review of Wholesale Mobile Wireless Services. Retrieved March 3, 2016, from http://www.crtc.gc.ca/eng/transcripts/2014/tt1001.htm

CRTC. (2014c, November 25). Transcript, Hearing 25 November 2014, Review of wholesale service and associated policies. Retrieved December 18, 2014, from http://www.crtc.gc.ca/eng/transcripts/2014/tt1125.htm

CRTC. (2014d, November 26). Transcript, Hearing 26 November 2014, Review of wholesale service and associated policies. Retrieved August 2, 2015, from http://www.crtc.gc.ca/eng/transcripts/2014/tt1126.htm

CRTC. (2014e, November 27). Transcript, Hearing 27 November 2014, Review of wholesale service and associated policies. Retrieved August 2, 2015, from http://www.crtc.gc.ca/eng/transcripts/2014/tt1127.htm

CRTC. (2014f, November 28). Transcript, Hearing 28 November 2014, Review of wholesale service and associated policies. Retrieved August 2, 2015, from http://www.crtc.gc.ca/eng/transcripts/2014/tt1128.htm

CRTC. (2014g, December 2). Transcript, Hearing 2 December 2014, Review of wholesale service and associated policies. Retrieved March 10, 2016, from http://www.crtc.gc.ca/eng/transcripts/2014/tt1202.htm

CRTC. (2015a, January 29). Broadcasting and Telecom Decision CRTC 2015-26. Retrieved May 14, 2016, from http://www.crtc.gc.ca/eng/archive/2015/2015-26.htm

CRTC. (2015b, February 12). Telecom Decision CRTC 2015-40. Retrieved April 4, 2016, from http://www.crtc.gc.ca/eng/archive/2015/2015-40.htm

CRTC. (2015c, April 9). Telecom Notice of Consultation CRTC 2015-134. Retrieved July 24, 2015, from http://www.crtc.gc.ca/eng/archive/2015/2015-134.htm

CRTC. (2015d, May 5). Telecom Regulatory Policy CRTC 2015-177. Retrieved May 9, 2016, from http://www.crtc.gc.ca/eng/archive/2015/2015-177.htm

CRTC. (2015e, July 22). Telecom Regulatory Policy 2015-326. Retrieved March 4, 2016, from http://www.crtc.gc.ca/eng/archive/2015/2015-326.htm

CRTC. (2015f, October 29). Communications Monitoring Report 2015. Retrieved April 2, 2016, from http://www.crtc.gc.ca/eng/publications/reports/PolicyMonitoring/2015/cmr.pdf

CRTC. (2016a, April 18). Transcript, Hearing April 18, 2016. Retrieved May 19, 2016, from http://www.crtc.gc.ca/eng/transcripts/2016/tt0418.htm

CRTC. (2016b, April 20). Transcript, Hearing April 20, 2016. Retrieved April 26, 2016, from http://www.crtc.gc.ca/eng/transcripts/2016/tt0420.htm

CRTC. (2016c, April 26). Transcript, Hearing April 26, 2016. Retrieved April 28, 2016, from http://www.crtc.gc.ca/eng/transcripts/2016/tt0426.htm

CRTC. (2016d, October 6). Telecom Order CRTC 2016-396. Retrieved October 7, 2016, from http://www.crtc.gc.ca/eng/archive/2016/2016-396.htm

CRTC. (2016e, November 1). Transcript, Hearing November 1, 2016. Retrieved November 2, 2016, from http://www.crtc.gc.ca/eng/transcripts/2016/tt1101.htm

CRTC. (2016f, December 21). Telecom Regulatory Policy CRTC 2016-496. Retrieved December 24, 2016, from http://www.crtc.gc.ca/eng/archive/2016/2016-496.htm

CRTC. (2017, April 20). Telecom Regulatory Policy CRTC 2017-104. Retrieved April 20, 2017, from http://crtc.gc.ca/eng/archive/2017/2017-104.htm

CRTC decision held a precedent for additional challenges to Bell. (1977, December 29). *Globe and Mail*, p. B2.

CRTC warned by Bell against being too free with data for public. (1976, October 26). *Globe and Mail*, p. B2.

CSEC. (2009). Cyber Threat Detection. Retrieved March 28, 2015, from https://www.christopher-parsons.com/Main/wp-content/uploads/2015/03/doc-5-cyber-csec-sdf-gchq-nov2009.pdf

CSEC. (2010). CSEC SIGINT Cyber Discovery: Summary of the current effort. Retrieved November 27, 2017, from http://www.spiegel.de/media/media-35665.pdf

CSEC. (2011a). CASCADE: Joint Cyber Sensor Architecture. Retrieved November 27, 2017, from https://www.documentcloud.org/documents/1690204-cascade-2011.html#document/p2

CSEC. (2011b). CSEC Cyber Threat Capabilities. Retrieved November 27, 2017, from https://s3.amazonaws.com/s3.documentcloud.org/documents/1690224/doc-6-cyber-threat-capabilities.pdf

CSEC. (2012a). IP Profiling Analytics & Mission Impacts. Retrieved November 27, 2017, from http://www.cbc.ca/news2/pdf/airports_redacted.pdf

CSEC. (2012b). Levitation and the FFU Hypothesis. Retrieved November 27, 2017, from https://s3.amazonaws.com/s3.documentcloud.org/documents/1510163/cse-presentation-on-the-levitation-project.pdf

CSEC. (2014). *Q&A prepared for the Chief in advance of his early February 2014 appearance at a Senate Security Committee* (ATI Request No. A-2014-0012). Retrieved November 27, 2017, from https://drive.google.com/file/d/0B0wdLKxvw1xsYzhKWVFJenlNWE0/edit?usp=sharing

CSIS. (2012). *All briefing notes to the Director and/or to the Minister concerning "Lawful Access" legislation for the period September 2011 to the present. Cabinet confidences should be excluded.* (ATI Request No. A-2011-114).

CSTAC. (2013, November 6). Security Best Practices for Canadian Telecommunications Service Providers (TSPs). Retrieved March 18, 2014, from http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10719.html

Curri, M. (n.d.). The South Dundas municipally-owned network: From fiber optic pioneer to cautionary tale. Retrieved November 27, 2017, from http://sngroup.com/wp-content/downloads/SNG_SouthDundas_16feb10.pdf

Cybera. (2013). *Cybera Strategic Plan 2013-2016*. Retrieved November 27, 2017, from http://www.cybera.ca/assets/Publications/2013-Cybera-Strategic-Report-online.pdf

Cybera. (2014a, November 24). Cybera's Presentation to the CRTC review of wholesale service and associated policies. Retrieved November 27, 2017, from http://www.cybera.ca/assets/Publications/Cybera-Presentation-CRTC-Hearing-Nov24-2014.pdf

Cybera. (2014b, December 11). Follow up on CRTC hearing on internet access. Retrieved December 11, 2014, from http://www.cybera.ca/news-and-events/tech-radar/follow-up-on-crtc-hearing-on-internet-access/

Cybera. (2014c, December 15). Alberta internet hub will drive down the cost of networking in the province.

Retrieved July 21, 2015, from http://www.cybera.ca/news-and-events/news/alberta-internet-hub-will-drive-down-the-cost-of-networking-in-the-province/

Cybera. (2015a, June 4). Open data on the rise as Albertans increase their use of public cloud computing. Retrieved July 16, 2015, from http://www.cybera.ca/news-and-events/news/albertas-cloud-computing-use-signals-the-rise-of-open-data-/

Cybera. (2015b, July 14). Final Submission of Cybera. Retrieved July 16, 2015, from http://www.cybera.ca/assets/Publications/CRTC-July14/Cybera-CRTC-2015-134-FinalSubmission.pdf

Cybera. (n.d.-a). Frequently Asked Questions. Retrieved July 14, 2015, from http://www.cybera.ca/about/cybera/faqs/#Whatiscybera

Cybera. (n.d.-b). President and CEO — Robin Winsor. Retrieved July 15, 2015, from http://www.cybera.ca/about/president-and-ceo/

Cybertip.ca. (2006, December 17). ISPs and Tipline Step Up Battle Against Internet Child Exploitation. Retrieved August 4, 2016, from http://web.archive.org/web/20061217184200/http://www.cybertip.ca/en/cybertip/cleanfeed_canada

Dagger, F. (1910). Is the Telephone a Natural Monopoly? *Canadian Municipal Journal*, *6*(1), 21–22.

Dagger, F. (1915). Public Ownership of Telephones in Canada. *Canadian Municipal Journal*, *11*(9), 308–309.

Davies, W. (2014). *The Limits of Neoliberalism: Authority, Sovereignty and the Logic of Competition*. Thousand Oaks, CA: SAGE.

de Beer, J. F., & Clemmer, C. D. (2009). Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries? *Jurimetrics*, *49*(4), 375–409.

de Raadt, T. (2013a). An Internet Exchange for Calgary. Retrieved November 27, 2017, from http://www.yycix.ca/talks/cuug-2013-06-18/an-internet-exchange-for-Calgary.pdf

de Raadt, T. (2013b, September 7). Re: AlbertaIX - no longer a Cybera project? *NANOG*. Retrieved July 21, 2015, from http://seclists.org/nanog/2013/Sep/157

Dean, M. (2007). *Governing Societies: Political Perspectives on Domestic and International Rule*. New York: Open University Press.

Dean, M. (2010). *Governmentality: Power and Rule in Modern Society* (2nd ed.). London: Sage.

DeBriyn, J. (2012). Shedding Light on Copyright Trolls: An Analysis of Mass Copyright Litigation in the Age of Statutory Damages. *UCLA Entertainment Law Review*, *19*(1). Retrieved November 27, 2017, from http://www.syfert.com/prenda-law-cases/AF_Holdings/mied.274202/gov.uscourts.mied.274202.12.2.pdf

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2008). *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: The MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2012). *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Cambridge, MA: The MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. L. (Eds.). (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: The MIT Press.

Deibert, R., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*(1), 15–32.

DeNardis, L. (2014). *The global war for internet governance*. Yale: Yale University Press.

Denton, T. (2013, October 1). Evolution of Canadian Telcom Policy 2008-2013. Retrieved December 2, 2014, from http://www.tmdenton.com/index.php/easyblog/entry/evolution-of-canadian-telcom-policy-2008-2013

Denton, T. (2014a, April 27). The contradiction at the heart of Canadian communications policy. Retrieved December 2, 2014, from http://www.tmdenton.com/index.php/easyblog/entry/the-contradiction-at-the-heart-of-canadian-communications-policy-1

Denton, T. (2014b, November 6). Ladders of investment roaming around. Retrieved December 4, 2014, from http://www.tmdenton.com/index.php/easyblog/entry/ladders-of-investment-roaming-around

Denton, T. (2016, November 17). Will JP get to use a nuke? Retrieved November 23, 2016, from http://www.tmdenton.com/index.php/easyblog/entry/will-jp-get-to-use-a-nuke

Dickson, F. (2015, January). Secure Pipes: Changing the Expectation of Your Internet Service Providers. Retrieved August 2, 2016, from http://securitysolutions.level3demandcenter.com/img/security_secure_pipes_frost_whitepaper.pdf

Distributel. (2013). Motion Record of Distributel Communications Limited. Retrieved November 27, 2017, from http://www.scribd.com/doc/124826637/Motion-Record-of-Distributel-Communications-Limited

Dobby, C. (2012, December 17). TekSavvy illegal downloading: Judge awards more time to warn clients. Retrieved November 27, 2017, from http://business.financialpost.com/2012/12/17/judge-gives-teksavvy-more-time-to-warn-customers-of-illegal-downloading-copyright-case/

Dobby, C. (2013, April 8). Shaw buys Calgary data firm to boost Internet muscle in $225M deal. Retrieved July 21, 2015, from http://business.financialpost.com/fp-tech-desk/shaw-buys-calgary-data-firm-to-boost-internet-muscle-in-225m-deal

Dobby, C. (2014a, January 2). How Canada’s telecom war turned ugly. Retrieved January 2, 2014, from http://business.financialpost.com/2014/01/02/how-canadas-telecom-war-turned-ugly/

Dobby, C. (2014b, July 16). Rogers now requires warrants for all police inquiries. Retrieved July 16, 2014, from http://www.theglobeandmail.com/report-on-business/rogers-now-requires-warrants-for-all-police-inquiries/article19634702/

Dobby, C. (2014c, September 30). Telus warns against ‘artificial’ competition within industry. Retrieved March 3, 2016, from http://www.theglobeandmail.com/report-on-business/telus-warns-against-artificial-competition-within-industry/article20871170/

Dobby, C. (2015a, January 29). Net neutrality: CRTC bans Bell from subsidizing data usage for mobile TV app. Retrieved February 22, 2015, from http://www.theglobeandmail.com/report-on-business/net-neutrality-crtc-bans-bell-from-subsidizing-data-usage-for-mobile-tv-app/article22696253/

Dobby, C. (2015b, February 6). Consumer groups challenge ‘tied selling’ of Cravetv, Shomi services. Retrieved February 6, 2015, from http://www.theglobeandmail.com/report-on-business/consumer-groups-challenge-tied-selling-of-cravetv-shomi-services/article22832759/

Dobby, C. (2015c, April 13). Bell Canada to revamp online ad program to allow upfront consent. Retrieved December 4, 2015, from http://www.theglobeandmail.com/report-on-business/bell-canada-to-revamp-online-ad-program-to-allow-upfront-consent/article23901505/

Dobby, C. (2015d, June 24). Mobilicity deal positions Wind to compete with wireless Big Three. Retrieved October 5, 2015, from http://www.theglobeandmail.com/report-on-business/mobilicity-deal-positions-wind-to-compete-with-big-three/article25101673/

Dobby, C. (2015e, October 20). CRTC rejects complaint about BCE's targeted ad program. Retrieved October 20, 2015, from http://www.theglobeandmail.com/report-on-business/crtc-rejects-complaint-about-bces-targeted-ad-program/article26888500/

Dobby, C. (2016a, January 14). Ontario court rules police orders breached cellphone users' Charter rights. Retrieved January 15, 2016, from http://www.theglobeandmail.com/report-on-business/industry-news/the-law-page/court-sides-with-telecoms-in-landmark-cellphone-privacy-case/article28180968/

Dobby, C. (2016b, April 18). CRTC chair makes strong call for national broadband strategy. Retrieved April 27, 2016, from http://www.theglobeandmail.com/report-on-business/crtc-chair-makes-strong-call-for-national-broadband-strategy/article29671174/

Dobson, C. (2016). *Regional Broadband Investigation: Municipal & Regional Opportunities & Options*. Calgary Regional Partnership. Retrieved November 27, 2017, from http://calgaryregion.ca/dam/Website/reports/General/Regional-economic-development/TWCL-Regnal-Broadband-Investigation-Municipal--Regional-Options-FINAL/TWCL-Regnal%20Broadband%20Investigation-Municipal%2C%20Regional%20Options-FINAL.pdf

Dobson, C., & Graham, J. (2016, May 10). Fibre Optic Broadband Provisioning. Retrieved February 5, 2017, from http://www.sprucegrove.org/Assets/pdf/reports/broadband_discuss_paper.pdf

Domingues, J. M. (1995). *Sociological theory and collective subjectivity*. London: Macmillan.

Douglas, M. (1966). *Purity and Danger: An analysis of the concepts of pollution and taboo*. London: Routledge and Kegan Paul.

Doyle, S. (2006). *Prey to Thievery: The Canadian Recording Industry Association and the Canadian Copyright Lobby, 1997 to 2005*. Ottawa: Simon Doyle.

Drahos, P., & Braithwaite, J. (2003). *Information Feudalism*. New York, N.Y.: New Press.

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, *15*(1), 105–122.

Dyrda, B. (2016). *Broadband for Economic and Community Development*. Presented at the Digital Futures 2016, Medicine Hat. Retrieved November 27, 2017, from https://drive.google.com/open?id=0B0jVqa4SGBfFcUpjblNlVHVQdXc

Eavesdropping on 'phones an offence. (1918, January 31). *Montreal Gazette*.

Eby, K. (2008, January 24). Role of ISPs thrown into copyright debate. Retrieved November 26, 2013, from http://www.thewirereport.ca/news/2008/01/24/role-of-isps-thrown-into-copyright-debate/18055

Edwards, L. (2011). *Role and responsibility of the internet intermediaries in the field of copyright and related rights* (Report). Geneva: WIPO. Retrieved November 27, 2017, from http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf

Eeten, M. J. G. van, & Bauer, J. M. (2008). *Economics of Malware: Security Decisions, Incentives and Externalities* (OECD Science, Technology and Industry Working Paper No. 2008/1). OECD Publishing. Retrieved November 27, 2017, from http://ideas.repec.org/p/oec/stiaaa/2008-1-en.html

Elder, J. (2002, March). *Orientation 2002*. Retrieved November 27, 2017, from http://www.ncf.ca/ncf/board/orientation/2002/Orientation.ppt

EORN. (n.d.). Open Access: A competitive internet marketplace. Retrieved September 26, 2016, from https://www.eorn.ca/en/resources/fact-sheets/20130513EN_EORN_FactSheet_EN_OpenAccess_Web.pdf

Everest, P. (2013, July 2). Interest in O-NET expands beyond Olds. Retrieved December 27, 2013, from http://www.oldsalbertan.ca/article/20130702/OLD0801/307029954/0/old

Everest, P. (2014a, January 28). Prominent mention on popular social media site brings O-NET and Olds wide attention. Retrieved February 4, 2014, from http://www.oldsalbertan.ca/article/20140128/OLD0801/301289955/0/old

Everest, P. (2014b, July 8). Problematic TV hardware, software prompts replacement effort for O-NET. Retrieved October 6, 2014, from http://www.oldsalbertan.ca/article/20140708/OLD0801/307089961/0/old

Faratin, P., Clark, D., Bauer, S., Lehr, W., Gilmore, P., & Berger, A. (2008). The Growing Complexity of Internet Interconnection. *Communications & Strategies*, *1*(72), 51–72.

Farivar, C. (2012, November 29). The rest of the Internet is too slow for Google Fiber. Retrieved February 11, 2014, from http://arstechnica.com/business/2012/11/the-rest-of-the-internet-is-too-slow-for-google-fiber/

FCC. (2015). Open Internet. Retrieved August 30, 2016, from https://www.fcc.gov/general/open-internet

Federation of Canadian Municipalities. (2009). Dealing with Telecom Companies: Protecting Municipal Rights of Way. Retrieved July 25, 2015, from https://www.fcm.ca/Documents/reports/Dealing_with_Telecom_Companies_Protecting_Municipal_Rights_of_Way_EN.pdf

Ferro, G. (2011, November 3). Show 72 - How We Are Killing the Internet. Retrieved February 19, 2014, from http://packetpushers.net/show-72-how-we-are-killing-the-internet/

Fiser, A., & Clement, A. (2012). A Historical Account of the Huh-ke-nah Network Broadband Deployment in a Remote Canadian Aboriginal Telecommunications Context. In A. Clement, M. Gurstein, G. Longford, A. Moll, & L. R. Shade (Eds.), *Connecting Canadians: Investigations in community informatics* (pp. 255–282). Edmonton: AU Press. Retrieved from http://www.aupress.ca/index.php/books/120193

Flam, H. (1990). Corporate actors: Definition, genesis, and interaction. *MPIFG Discussion Paper*. Retrieved November 27, 2017, from http://www.mpifg.de/pu/mpifg_dp/dp90-11.pdf

Flichy, P. (2007). *The Internet Imaginaire*. (L. Carey-Libbrecht, Trans.). Cambridge, MA: MIT Press.

Forcese, C. (2013, November 22). Bill C-13: Does the Trojan Horse Contain Lawful Access Gifts, or Just Greek Hoplites - National Security Law Blog -. Retrieved December 16, 2013, from http://craigforcese.squarespace.com/national-security-law-blog/2013/11/22/bill-c-13-does-the-trojan-horse-contain-lawful-access-gifts.html

Foucault, M. (1982). The subject and power. *Critical Inquiry*, *8*(4), 777–795.

Foucault, M. (2007). *Security, Territory, Population: Lectures at the College de France, 1977-78*. (G. Burchell, Trans.). New York: Palgrave Macmillan.

Fraser, D. (2011, November 5). Canadian Privacy Law Blog: Dealing with police "Letters of Request for Information." Retrieved January 2, 2014, from http://blog.privacylawyer.ca/2011/11/dealing-with-police-letters-of-request.html

Fraser, D. (2016, January 18). Tower dump case raises troubling questions about law enforcement and privacy. Retrieved February 4, 2016, from http://blog.privacylawyer.ca/2016/01/tower-dump-case-raises-troubling.html

Fraser, F. (2008, October 1). Only So Super. Retrieved April 8, 2015, from http://albertaventure.com/2008/10/only-so-super/

Fraser, M. (1999). *Free-For-All: The Struggle for Dominance on the Digital Frontier*. Toronto: Stoddart.

Freeman, S. (2013, October 8). Indie ISPs Accuse Big Telecom Of "Anti-Competitive Behaviour." Retrieved October 9, 2013, from http://www.huffingtonpost.ca/2013/10/08/internet-providers-crtc-complaint_n_4066240.html

Freeze, C. (2014, January 22). Telecom firms being asked what data they are giving to police, intelligence agencies. Retrieved January 25, 2014, from http://www.theglobeandmail.com/news/national/telecom-firms-being-asked-what-data-they-are-giving-to-police-intelligence-agencies/article16455076/

Freeze, C., Dobby, C., & Wingrove, J. (2014, June 5). TekSavvy, Rogers break silence over government requests for data. Retrieved June 7, 2014, from http://www.theglobeandmail.com/technology/tech-news/teksavvy-opens-books-on-government-data-requests/article18999107/

Freeze, C., & Trichur, R. (2013, September 16). Wireless firms rejected Ottawa's changes to surveillance rules over cost concerns. Retrieved September 17, 2013, from http://www.theglobeandmail.com/technology/mobile/wireless-firms-reject-ottawas-changes-to-surveillance-rules-over-cost-concerns/article14363379/

Frieden, R. (2005). Lessons from broadband development in Canada, Japan, Korea and the United States. *Telecommunications Policy*, *29*(8), 595–613.

Fulk, J., Flanagin, A. J., Kalman, M. E., Monge, P. R., & Ryan, T. (1996). Connective and Communal Public Goods in Interactive Communication Systems. *Communication Theory*, *6*(1), 60–87.

Fung, B. (2016, January 20). Internet providers want to know more about you than Google does, privacy groups say. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2016/01/20/your-internet-provider-is-turning-into-a-data-hungry-tech-company-consumer-groups-warn/

Gall, K. (2015, May 29). Internet speed in Olds drawing a crowd. Retrieved July 7, 2015, from http://calgaryherald.com/life/swerve/would-you-move-to-the-town-of-olds-for-its-gigabit-age-internet-speed

Gallagher, S. (2012, August 29). Big brother on a budget: How internet surveillance became so cheap. Retrieved December 21, 2015, from http://www.wired.co.uk/news/archive/2012-08/29/dpi-internet-surveillance

Galloway, A. R. (2004). *Protocol: How Control Exists After Decentralization*. Cambridge, MA: MIT Press.

Gaudrault, M. (2012a, December 14). Discussion about log retention. *DSLReports Forums: TekSavvy*. Retrieved November 27, 2017, from http://www.dslreports.com/forum/r27824502-Discussion-about-log-retention

Gaudrault, M. (2012b, December 15). Why we are not opposing motion on Monday. *DSLReports Forums: TekSavvy*. Retrieved December 18, 2012, from http://www.dslreports.com/forum/r27824891-Why-we-are-not-opposing-motion-on-Monday.

Geist, M. (Ed.). (2005). *Internet and E-Commerce Law in Canada*, *6*(5). Retrieved November 27, 2017, from http://www.macerajarzyna.com/pages/publications/BMG%20Case%20-%20E-Commerce.pdf

Geist, M. (2011). Canada’s Usage Based Billing Controversy: How to Address the Wholesale and Retail Issues. *Queen’s Law Journal*, *37*(1), 221–256.

Geist, M. (2012a, February 13). Everything You Always Wanted to Know About Lawful Access, But Were (Understandably) Afraid To Ask. Retrieved November 2, 2015, from http://www.michaelgeist.ca/2012/02/lawful-access-faq/

Geist, M. (2012b, May 22). How Canada’s Telecom Companies Have Secretly Supported Internet Surveillance Legislation. Retrieved November 4, 2012, from http://www.michaelgeist.ca/content/view/6505/135/

Geist, M. (2013a, October 8). Canadian Government Quietly Pursuing New ISP Code of Conduct. Retrieved October 9, 2013, from http://www.michaelgeist.ca/content/view/6964/159/

Geist, M. (2013b, November 21). Lawful Access is Back: Controversial Bill Returns Under the Guise of Cyber-Bullying Legislation. Retrieved November 21, 2013, from http://www.michaelgeist.ca/content/view/7003/125/

Geist, M. (2014a, April 4). Federal government shows it’s interested in digital issues, but lacks a big-picture goal. *The Toronto Star*. Retrieved November 27, 2017, from http://www.thestar.com/business/2014/04/04/digital_canada_150_the_digital_strategy_without_a_strategy.html

Geist, M. (2014b, June 17). Government Rejects Supreme Court Privacy Decision: Claims Ruling Has No Effect on Privacy Reform. Retrieved November 15, 2015, from http://www.michaelgeist.ca/2014/06/government-rejects-spencer-on-s-4/

Geist, M. (2014c, November 7). The Big 3 carriers argue that the Canadian market is too small to support a fourth national carrier. But the government and a major OECD study say otherwise. *The Toronto Star*. Retrieved

November 27, 2017, from http://www.thestar.com/business/2014/11/07/why_canada_needs_a_fourth_wireless_player.html

Geist, M. (2015, January 9). Canadian ISPs Responding to Copyright Notices By Adding Information on Notice System, Privacy Concerns. Retrieved January 13, 2015, from http://www.michaelgeist.ca/2015/01/canadian-isps-responding-copyright-notices-adding-information-notice-system-privacy-concerns/

Geist, M. (2016a, January 12). The Battle Over the Future of Broadband in Canada: Mayors Tory & Watson v. Nenshi. Retrieved January 12, 2016, from http://www.michaelgeist.ca/2016/01/the-battle-over-the-future-of-broadband-in-canada-mayors-tory-watson-v-nenshi/

Geist, M. (2016b, January 25). Why your telecom must defend your right to privacy. *The Toronto Star*. Retrieved November 27, 2017, from http://www.thestar.com/business/2016/01/25/why-your-telecom-must-defend-your-right-to-privacy-geist.html

Geist, M. (2017, April 3). Why warrantless access to Internet information is back on the lawmaking agenda. Retrieved April 4, 2017, from http://www.theglobeandmail.com/report-on-business/rob-commentary/why-warrantless-access-to-internet-information-is-back-on-the-lawmaking-agenda/article34567424/

Geng, X., & Whinston, A. B. (2000). Defeating distributed denial of service attacks. *IT Professional*, *2*(4), 36–42.

Giddens, A. (1984). *The Constitution of Society: Outline of the Theory of Structuration*. Cambridge, U.K.: Polity Press.

Gignac, T. (2003, March 10). Learning Live: The SuperNet's high-speed promise. *Calgary Herald*, p. 10.

Gignac, T. (2010, August 22). SuperNet's digital dream still out of reach for rural Alberta. Retrieved April 25, 2013, from http://www2.canada.com/calgaryherald/news/story.html?id=4bac9195-673f-4dbf-b817-6fc5750496de&p=3

Gignac, T. (2011, November 7). Broadband service for rural Alberta a priority with premier. *Edmonton Journal*, p. A4.

Gignac, T. (2013, July 23). Superfast web service puts Olds on world map. *Canada.Com*. Retrieved November 27, 2017, from http://www.canada.com/news/alberta/Superfast+service+puts+Olds+world/8703980/story.html

Gilbert, M. (2014). *Joint Commitment: How We Make the Social World*. Oxford: Oxford University Press.

Goetz, S. (2014, February 10). Mayor Kraemer: Selling Bruce Telecom the best of bad option. Retrieved August 4, 2015, from http://www.kincardinenews.com/2014/02/10/mayor-kraemer-selling-bruce-telecom-the-best-of-bad-options

Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet?: Illusions of a borderless world*. Oxford: Oxford University Press.

Gómez-Barroso, J. L., & Feijóo, C. (2010). A conceptual framework for public-private interplay in the telecommunications sector. *Telecommunications Policy*, *34*(9), 487–495.

Goodyear, S. (2016, February 8). CRTC will soon have to decide whether home internet access is a Canadian right. Retrieved March 6, 2016, from http://www.cbc.ca/news/technology/internet-access-digital-divide-

1.3433848

Government of Alberta. (2005, February 22). Government of Alberta, Axia, and Bell Canada announce SuperNet completion plan. Retrieved November 27, 2017, from http://www.gov.ab.ca/release.cfm?xID=176189D55D0E4-366F-4D8C-92CFEC9A8BC75236

Government of Alberta. (2012, March 19). High-speed Internet access coming to unserviced rural areas. Retrieved April 24, 2015, from http://alberta.ca/release.cfm?xID=321362C133FA2-D71D-86CB-6C4D2EA8BD019B22

Government of Alberta, Axia Netmedia, & Bell Canada. (n.d.). Harnessing the SuperNet Advantage. Retrieved from http://www.bell.ca/media/en/all_regions/pdf/business/SuperNet_v4.pdf

Government of Alberta, Bell Canada, & Axia SuperNet Ltd. (2005, June 30). Amended and Restated SuperNet Master Agreement.

Government of Canada. Bell Telephone Company of Canada Act (1880).

Government of Canada. An Act to amend Act incorporating "The Bell Telephone Company of Canada" (1882).

Government of Canada. Telecommunications Act (1993). Retrieved from http://laws-lois.justice.gc.ca/eng/acts/T-3.4/

Government of Canada. (1996, August 6). Convergence Policy Statement. Retrieved August 9, 2015, from https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf05265.html

Government of Canada. Personal Information Protection and Electronic Documents Act (2000). Retrieved November 27, 2017, from http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

Government of Canada. (2002, August 25). Lawful Access – Consultation Document. Retrieved October 4, 2014, from http://www.justice.gc.ca/eng/cons/la-al/consult.html

Government of Canada. (2006, December 14). Order Issuing a Direction to the CRTC on Implementing the Canadian Telecommunications Policy Objectives. Retrieved November 27, 2017, from http://laws-lois.justice.gc.ca/eng/regulations/SOR-2006-355/page-1.html

Government of Canada. Toronto — Round Table and Public Hearings on Copyright (2009). Retrieved November 27, 2017, from http://web.archive.org/web/20130702171814/http://www.ic.gc.ca/eic/site/008.nsf/eng/h_04034.html

Government of Canada. (2012). Copyright Modernization Act. Retrieved July 10, 2014, from http://laws-lois.justice.gc.ca/eng/annualstatutes/2012_20/FullText.html

Government of Canada. (2013a, March 7). Harper Government Puts Consumers First in Telecommunications Plan. Retrieved April 11, 2016, from http://news.gc.ca/web/article-en.do?nid=724349

Government of Canada. (2013b, June 5). Speech from the Throne. Retrieved November 27, 2017 from https://lop.parl.ca/ParlInfo/Documents/ThroneSpeech/41-2-e.html

Government of Canada. (2014). Digital Canada 150. Retrieved April 20, 2015, from https://www.ic.gc.ca/eic/site/028.nsf/eng/h_00569.html

Government of Canada. (2016, May 11). Statement by the Government of Canada on Bell Canada petition of CRTC wholesale decision. Retrieved May 11, 2016, from http://news.gc.ca/web/article-en.do?nid=1063779

Government of Canada, P. S. C. (2015, June 19). Cyber security. Retrieved July 1, 2015, from http://www.canada.ca/en/services/defence/cybersecurity/index.html

Graham, G. (2011). Towards a National Strategy for Digital Inclusion: Addressing Social and Economic Disadvantage in an Internet Economy. In M. Moll & L. R. Shade (Eds.), *The Internet Tree: The State of Telecom Policy in Canada 3.0* (p. 29-). Ottawa: Canadian Centre for Policy Alternatives. Retrieved November 27, 2017, from http://www.policyalternatives.ca/sites/default/files/uploads/publications/National%20Office/2011/06/Internet_Tree_0.pdf

Graham, M. (2013). Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities? *The Geographical Journal*, *179*(2), 177–182.

Griffin, S., Simard, A.-E., & Bellefleur, M. (2015, February 25). Bill C-13: Lawful Access and the Relationship Between Organizations, Cyber-bullying and the Protection of Privacy Rights. Retrieved February 3, 2016, from http://www.canadiantechlawblog.com/2015/02/25/bill-c-13-lawful-access-and-the-relationship-between-organizations/

Gurstein, M. (2003). Effective use: A community informatics strategy beyond the Digital Divide. *First Monday*, *8*(12). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/1107

Gustafson, J., & McInnis, N. (2016). *Town of Olds broadband presentation*. Retrieved November 27, 2017, from https://www.youtube.com/watch?v=Z0WPRCaQv6A

Hafner, K., & Lyon, M. (1996). *Where wizards stay up late*. New York: Simon & Schuster.

Haggart, B. (2014). *Copyfight: The Global Politics of Digital Copyright Reform*. Toronto: University of Toronto Press.

Handa, S., Birbilas, L., & Fazio, J. D. (2015, January 23). Bill C-13: Cyberbullying Bill Introduces New Lawful Access Measures. Retrieved February 3, 2016, from http://www.blakes.com/English/Resources/Bulletins/Pages/Details.aspx?BulletinID=2057

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

Harnisch, S. (2011). Role theory: Operationalization of key concepts. In S. Harnisch, C. Frank, & H. W. Maull (Eds.), *Role Theory in International Relations* (pp. 7–15). London: Routledge.

Harvey, D., & Morozov, E. (2016, November). *David Harvey on post-neoliberalism, Trump, infrastructure, sharing economy, smart city*. Barcelona. Retrieved November 27, 2017, from https://www.youtube.com/watch?v=wb6rhHyJJ_4

Hawkins, K. (1992). The Uses of Legal Discretion: Perspective from Law and Social Science. In K. Hawkins (Ed.), *The Uses of Discretion* (pp. 11–46). Oxford: Clarendon Press.

Hay, M. (2013, August 23). RE: Vancouver IXP - VanTX - BCNet. *NANOG*. Retrieved December 4, 2013, from http://seclists.org/nanog/2013/Aug/457

Hecht, J. (2015, February 12). Net Neutrality's Technical Troubles - IEEE Spectrum. Retrieved February 22, 2015, from http://spectrum.ieee.org/telecom/internet/net-neutralitys-technical-troubles/

Henderson, P. (2014a, April 30). Bell defends targeted ad program as 'transparent.' Retrieved May 1, 2014, from http://www.thewirereport.ca/news/2014/04/30/bell-defends-targeted-ad-program-as-%E2%80%98transparent%E2%80%99/28217

Henderson, P. (2014b, August 21). PIPEDA complaints double, many target Bell's tracking program. Retrieved September 13, 2014, from http://www.thewirereport.ca/news/2014/08/21/pipeda-complaints-double-many-target-bells-tracking-program/28666

Henderson, P. (2014c, November 25). Small ISPs tell CRTC they want to invest in 'middle mile.' Retrieved November 25, 2014, from http://www.thewirereport.ca/news/2014/11/25/small-isps-tell-crtc-they-want-to-invest-in-%E2%80%98middle-mile%E2%80%99/29014

Henderson, P., & Karadeglija, A. (2014, July 31). CRTC finds Rogers' treatment of Wind Mobile 'unjust.' Retrieved September 13, 2014, from http://www.thewirereport.ca/news/2014/07/31/crtc-finds-rogers%E2%80%99-treatment-of-wind-mobile-%E2%80%98unjust%E2%80%99/28609

Hildebrand, J. (2014, January 15). Erosion of the moral authority of transparent middleboxes. Retrieved February 8, 2015, from https://tools.ietf.org/html/draft-hildebrand-middlebox-erosion-00

Hilvert, J. (2010, December 1). ISPs sign up to voluntary anti-zombie code. Retrieved January 10, 2013, from http://www.itnews.com.au/News/240285,isps-sign-up-to-voluntary-anti-zombie-code.aspx

Ho, J. (2014, February 25). O-NET seeks approval for $8-million loan. Retrieved February 25, 2014, from http://www.oldsalbertan.ca/article/20140225/OLD0801/302259966/-1/old/o-net-seeks-approval-for-8-million-loan

Hoffman, P. (2012). The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force. Retrieved September 5, 2013, from http://www.ietf.org/tao.html

Horten, M. (2012). *The Copyright Enforcement Enigma: Internet Politics and the "Telecoms Package."* New York: Palgrave Macmillan.

Houle, G. (2016). Gaétan Houle. Retrieved September 15, 2016, from https://ca.linkedin.com/in/ga%C3%A9tan-houle-1005102

House of Commons. (2012, February 13). House of Commons Debates. Retrieved November 23, 2016, from http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&Parl=41&Ses=1&DocId=5380035

House of Commons of Canada. (2012, February 14). Bill C-30, First Reading (41-1). Retrieved November 27, 2017, from http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=5380965&File=4

House of Commons Standing Committee on Access to Information, Privacy and Ethics. (2007, February 13). Transcript of meeting no. 30, February 13, 2007. Retrieved November 1, 2015, from http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=2695445&Language=E&Mode=1

House of Commons Standing Committee on Industry, Science and Technology. (2011, February 10). Transcript, Standing Committee on Industry, Science and Technology, Thursday, February 10, 2011. Retrieved June 4, 2013, from http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=4953635&Language=E&Mode=1

Hovis, J. (2013, April). The Business Case For Government Fiber Networks. *Broadband Communities*, 60–63.

Howard, P. N., Busch, L., & Sheets, P. (2010). Comparing Digital Divides: Internet Access and Social Inequality in Canada and the United States. *Canadian Journal of Communication*, *35*(1). Retrieved November 27, 2017, from http://www.cjc-online.ca/index.php/journal/article/view/2192

Hubbard, R. W., Brauti, P. M., & Fenton, S. K. (2015). *Wiretapping and Other Electronic Surveillance: Law and Procedure*. Toronto: Thomson Reuters.

Hubbard, R. W., Magotiaux, S., & Proestos, X. (2002). Limits of Privacy: Police Access to Subscriber Information in Canada, The. *Criminal Law Quarterly*, *46*, 361.

Hunt, A. (Ed.). (2014). *In Their Own Words: The Story of National Capital FreeNet* (3rd ed.). Retrieved November 27, 2017, from http://web.ncf.ca/fn352/InTheirOwnWords.pdf

Ibbitson, J. (2012, May 15). How the Toews-sponsored Internet surveillance bill quietly died. Retrieved July 7, 2012, from http://www.theglobeandmail.com/news/politics/how-the-toews-sponsored-internet-surveillance-bill-quietly-died/article4179310/

IETF 88 perpass "BoF" session. (2013). Vancouver. Retrieved November 27, 2017, from http://www.ietf.org/audio/ietf88/ietf88-regencyd-20131106-1300-pm3.mp3

Industry Canada. (1994). *The Canadian Information Highway* (Cat. No. C2-229/1994E).

Industry Canada. (2007). Spectrum Policy Framework for Canada. Retrieved January 27, 2017, from https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/spf2007e.pdf/$FILE/spf2007e.pdf

Industry Canada. (2012). *Memos, decks and briefing notes since January 1, 2006, whose main topic is the issue of "Lawful Access" by Canadian police and security agencies to customer data held by Canadian telecommunications companies held by the Strategic Policy Sectory.* (ATI Request No. A-2007-00169). Retrieved from http://www.scribd.com/doc/79972705/Industry-Canada-documents-on-Lawful-Access-c-2006

Industry Canada. (2013). *Reports, presentation, and memos relating to the Canadian Telecommunications Cyber Protection Working Group (CTCP), as well as minutes and meeting summaries from CTCP meetings. From January 1, 2012 to July 1, 2013* (ATI Request No. A-2013-00189).

Industry Canada. (2014a). *Documents and correspondence pertaining to the founding of the Canadian Security Telecommunications Advisory Committee (CSTAC), as well as minutes, meeting summaries, and presentations from CSTAC meetings, from September 1, 2010 to the present (July 10, 2013)* (ATI Request No. A-2013-00188).

Industry Canada. (2014b). *Lawful Intercept alterations re: impacts to wireless and internet providers — January 1, 2010 to March 1, 2013* (ATI Request No. A-2012-00175).

Industry Canada. (2014c, July 22). Harper Government launches program to bring high-speed Internet to an additional 280,000 Canadian households. Retrieved November 27, 2017, from https://web.archive.org/web/20150522203642/http://news.gc.ca/web/article-en.do?nid=869539

Industry Canada. (2015, June 30). Transparency Reporting Guidelines. Retrieved December 4, 2017, from http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html

Information Highway Advisory Council. (1995). *Connection, Community, Content: The Challenge of the Information Highway*. Ottawa: Industry Canada.

Information Highway Advisory Council. (1996). *Building the Information Society: Moving Canada in the 21st Century*. Ottawa: Government of Canada.

Information Highway Advisory Council. (1997). *Preparing Canada for a Digital World*. Ottawa: Industry Canada.

ISED. (2016). *Any documents pertaining to Telecommunication Services Provider Security Best Practices, as well as minutes, meeting summaries, and presentations from CSTAC meetings, from July, 2013 to the present (December 2, 2014)* (ATI Request No. A-2014-00421).

ISP Summit. (2013). *Regulatory Panel: What's Cooking in Ottawa*. Retrieved December 4, 2017, from https://www.youtube.com/watch?v=RN_yB7HAAPg

ISPs Put the Boots to Telco. (n.d.). Retrieved December 4, 2017, from https://www.hackcanada.com/telco/canuck/agt.html

Israel, T. (2012, March 23). Bill C-12: Safeguarding Canadians' Personal Information Act – eroding privacy in the name of privacy. Retrieved December 4, 2017, from http://www.slaw.ca/2012/03/23/billc12-safeguarding-privacy-by-eroding-it/

Jackson, E. (2016a, November 24). Telus aims to bridge digital divide with $9.95 Internet for low-income families in Alberta. Retrieved November 25, 2016, from http://business.financialpost.com/fp-tech-desk/telus-aims-to-bridge-digital-divide-with-9-95-internet-for-low-income-families-in-alberta

Jackson, E. (2016b, December 9). CRTC says it holds power over website blocking in Quebec gambling case. Retrieved March 11, 2017, from http://business.financialpost.com/fp-tech-desk/crtc-says-it-can-force-quebec-to-unblock-gambling-websites

Jackson, E. (2017a, February 15). BCE Inc. receives final approval to buy MTS in $3.9-billion deal, Xplornet enters Manitoba market. Retrieved March 23, 2017, from http://business.financialpost.com/fp-tech-desk/bce-inc-receives-final-approval-to-buy-manitoba-telecom-services-in-3-9-billion-deal

Jackson, E. (2017b, March 3). Left in the digital dark ages, small town Canada chases its own gigabit dream. Retrieved March 4, 2017, from http://business.financialpost.com/fp-tech-desk/left-in-the-digital-dark-ages-small-town-canada-chases-its-own-gigabit-dream

Janisch, H. N. (1979). Policy making in regulation: towards a new definition of the status of independent regulatory agencies in Canada. *Osgoode Hall Law Journal*, *17*(1), 46–106.

Janisch, H. N., & Schultz, R. J. (1991). Federalism's Turn: Telecommunications and Canadian Global Competitiveness. *Canadian Business Law Journal*, *18*(2), 161–187.

John, R. R. (2010). *Network Nation: Inventing American Telecommunications*. Cambridge, MA: Belknap Press.

Johnston, L., & Shearing, C. D. (2003). *Governing Security: Explorations of Policing and Justice: Explorations in Policing and Justice*. New York: Routledge.

Joselyn, B. (2013, December). Broadband Adoption and Economic Opportunity. *Broadband Communities*. Retrieved December 4, 2017 from http://www.bbpmag.com/2013mags/november/BBC_Nov13_BroadbandAdoption.pdf

Karadeglija, A. (2014a, April 15). Jury out on what Digital Privacy Act does to privacy, copyright. Retrieved April 17, 2014, from http://www.thewirereport.ca/news/2014/04/15/jury-out-on-what-digital-privacy-act-does-to-privacy-copyright/28141

Karadeglija, A. (2014b, May 2). Telecoms don’t give out customer info ‘willy-nilly’: Bell ombudsman. Retrieved May 6, 2014, from http://www.thewirereport.ca/news/2014/05/02/telecoms-don%E2%80%99t-give-out-customer-info-%E2%80%98willy-nilly%E2%80%99-bell-ombudsman/28229

Karadeglija, A. (2014c, June 18). Has the time come to make broadband a basic service? Retrieved June 19, 2014, from http://www.thewirereport.ca/news/2014/06/18/has-the-time-come-to-make-broadband-a-basic-service/28438

Karadeglija, A. (2015a, March 31). Telecom and broadcasting converge as legislation remains separate. Retrieved March 31, 2015, from http://www.thewirereport.ca/news/2015/03/31/telecom-and-broadcasting-converge-as-legislation-remains-separate/29451

Karadeglija, A. (2015b, June 30). ‘Arbitrary’ limits in Industry Canada transparency guidelines: critics. Retrieved June 30, 2015, from http://www.thewirereport.ca/news/2015/06/30/%E2%80%98arbitrary%E2%80%99-limits-in-industry-canada-transparency-guidelines-critics/29799

Karadeglija, A., & Shekar, S. (2015, July 22). UPDATED: ‘Good day’ for small ISPs as CRTC mandates FTTH access. Retrieved July 23, 2015, from http://www.thewirereport.ca/news/2015/07/22/crtc-mandates-%E2%80%98disaggregated%E2%80%99-wholesale-access-includes-ftth/29877

Kaul, I., & Mendoza, R. U. (2003). Advancing the concept of public goods. In I. Kaul, P. Conceição, K. L. Goulven, & R. U. Mendoza (Eds.), *Providing global public goods: Managing globalization* (pp. 78–111). Oxford: Oxford University Press.

Kerr, I., & Cameron, A. (2006). NYMITY, P2P & ISPS: Lessons from BMG Canada Inc. v. John Doe. In K. J. Strandburg & D. S. Raicu (Eds.), *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation* (p. 269-). New York: Springer.

Kerr, I., & Gilbert, D. (2004). The Role of ISPs in the Investigation of Cybercrime. In T. Mendina & J. J. Britz (Eds.), *Information Ethics in the Electronic Age: Current Issues in Africa and the World* (pp. 163–172). Jefferson, N.C.: Mcfarland & Company.

Kinsman, G., Buse, D. K., & Steedman, M. (2000). How the Centre Holds: National Security as an Ideological Practicce. In G. Kinsman, D. K. Buse, & M. Steedman (Eds.), *Whose National Security?: Canadian State Surveillance and the Creation of Enemies* (pp. 278–285). Toronto: Between the Lines.

Klass, B. (2013, November 20). Crossing the Line. Retrieved December 4, 2017, from http://benklass.wordpress.com/2013/11/20/crossing-the-line/

Knopf, H. (2013, January 8). Mass Copyright Litigation in Canada: Some Observations on the Roles and Responsibilities of ISPs and their Customers. Retrieved January 10, 2013, from http://excesscopyright.blogspot.ca/2013/01/mass-copyright-litigation-in-canada.html

Knopf, H. (2015, November 8). TekSavvy's Appeal to Get $346,480.68 for Taking the Position to Take "No Position" - "Nice Work If You Can Get It"? Retrieved November 30, 2015, from http://excesscopyright.blogspot.ca/2015/11/teksavvys-appeal-to-get-34648068-for.html

Kozak, N. I. (2010). *On the last mile : the effects of telecommunications regulation and deregulation in the rural western United States and Canada* (dissertation). Retrieved December 4, 2017, from http://escholarship.org/uc/item/8nv621sn

Kozak, N. I. (2013). Local Communities and Home Rule: Extending the Alberta SuperNet to Unserved Areas. *The Journal of Community Informatics*, *10*(2). Retrieved December 4, 2017, from http://ci-journal.net/index.php/ciej/article/view/1002

Krajewski, P. (2017, July 17). Shaw connects town to high-speed future. Retrieved September 24, 2017, from http://www.highrivertimes.com/2017/07/17/shaw-connects-town-to-high-speed-future

Krashinsky, S. (2011, March 1). CRTC's Internet decision "simply wrong," Clement says. Retrieved February 23, 2015, from http://www.theglobeandmail.com/technology/tech-news/crtcs-internet-decision-simply-wrong-clement-says/article568826/

Kushida, K. E. (2015). The Politics of Commoditization in Global ICT Industries: A Political Economy Explanation of the Rise of Apple, Google, and Industry Disruptors. *Journal of Industry, Competition and Trade*, 1–19.

Kyonka, N. (2013a, October 1). Small ISPs say cablecos "unduly discriminating" against them. Retrieved October 12, 2013, from http://www.thewirereport.ca/news/2013/10/01/small-isps-say-cablecos-%E2%80%98unduly-discriminating%E2%80%99-against-them/27318

Kyonka, N. (2013b, November 4). NGN, Riding drop filesharing case against Distributel. Retrieved November 5, 2013, from http://www.thewirereport.ca/news/2013/11/04/ngn-riding-drop-filesharing-case-against-distributel/27460

Kyonka, N. (2014, February 10). Rules could stymie inquiry of telecoms' info disclosure to government. Retrieved February 11, 2014, from http://www.thewirereport.ca/news/2014/02/10/rules-could-stymie-inquiry-of-telecoms%E2%80%99-info-disclosure-to-government/27839

Kyonka, N., & Doyle, S. (2012, March 14). Caps on 'prime' 700 MHz spectrum, no foreign ownership rules for small players, Industry Canada says. Retrieved March 16, 2015, from http://www.thewirereport.ca/news/2012/03/14/caps-on-%E2%80%98prime%E2%80%99-700-mhz-spectrum-no-foreign-ownership-rules-for-small-players-industry/23655

Labovitz, C., Iekel-Johnson, S., McPherson, D., Oberheide, J., & Jahanian, F. (2010). Internet Inter-Domain Traffic. Presented at the SIGCOMM'10, New Delhi. Retrieved December 4, 2017, from https://jon.oberheide.org/files/sigcomm10-interdomain.pdf

LaFrance, A. (2014, June 10). The Promise of a New Internet. *The Atlantic*. Retrieved December 4, 2017, from http://www.theatlantic.com/technology/archive/2014/06/the-promise-of-an-alternative-internet/372501/

Larsen, M., & Walby, K. (Eds.). (2012). *Brokering Access: Power, Politics, and Freedom of Information Process in Canada*. Vancouver: UBC Press.

Lawson, P. (2011, November 23). Bill C-12 and "lawful authority" under PIPEDA. Retrieved December 4, 2017, from http://www.slaw.ca/2011/11/23/bill-c-12-and-lawful-authority/

Lawson, P., & O'Donoghue, M. (2009). Approaches to Consent in Canadian Data Protection Law. In I. Kerr, C. Lucock, & V. Steeves (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 399–416). Oxford: Oxford University Press.

Leafloor, B. (2004, October). *Assuring Telecom (Infrastructure and Services): An Operations Perspective*. Retrieved December 4, 2012, from http://www.isacc.ca/isacc/_doc/ArchivedPlenary/TSACC-04-32302.pdf

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., … Wolff, S. (2009). A Brief History of the Internet. *SIGCOMM Computer Communication Review*, *39*(5), 22–31.

Lemley, M. A., & Lessig, L. (2001). The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era. *UCLA Law Review*, *48*(4), 925–972.

Levi-Faur, D. (1999). The Governance of Competition: The Interplay of Technology, Economics, and Politics in European Union Electricity and Telecom Regimes. *Journal of Public Policy*, *19*(2), 175–207.

Levi-Faur, D. (2006). Regulatory Capitalism: The Dynamics of Change beyond Telecoms and Electricity. *Governance*, *19*(3), 497–525.

Lie, E. (2003). Promoting Broadband: The Case of Canada. International Telecommunication Union. Retrieved December 4, 2017, from https://www.itu.int/osg/spu/ni/promotebroadband/casestudies/canada.pdf

Ling, J. (2014, May 15). For Canada's Spies, Your Data Is Just a Phone Call Away. Retrieved February 4, 2015, from http://motherboard.vice.com/read/canadian-spies-can-look-at-your-user-data-consequence-free

Ling, J. (2015, January 20). The RCMP Spent $1.6 Million to Run an Unconstitutional Spying Program. Retrieved January 22, 2015, from http://www.vice.com/en_ca/read/the-rcmp-spent-16-million-to-run-an-unconstitutional-spying-program-239

Linton, W. (2002, March 25). Regulatory reform next step in ensuring sustainable competition, Call-Net says. Retrieved October 21, 2015, from http://www.thewirereport.ca/news/2002/03/25/regulatory-reform-next-step-in-ensuring-sustainable-competition-call-net-says/14528

Lithwick, D. (2014a, June 11). Legislative Summary of Bill S-4: An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act. Retrieved December 4, 2017, from http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/41/2/s4-e.pdf

Lithwick, D. (2014b, November 25). R. v. Spencer, Internet Privacy and Parliament. Retrieved December 4, 2017, from https://hillnotes.wordpress.com/2014/11/25/r-v-spencer-internet-privacy-and-parliament/

Little, D. (2013, October 5). Understanding Society: Issues about microfoundations. Retrieved December 4, 2017, from http://understandingsociety.blogspot.ca/2013/10/issues-about-microfoundations.html

Little, D. (2014, December 29). John Levi Martin on theory. Retrieved December 4, 2017, from http://understandingsociety.blogspot.ca/2014/12/john-levi-martin-on-theory.html

Longford, G. (2007). Download This! Contesting Digital Rights in a Global Era: The Case of Music Downloading in Canada. In *How Canadians Communicate II: Media, Globalization, and Identity* (pp. 195–216). Calgary: University of Calgary Press.

Longford, G., Clement, A., Gurstein, M., & Shade, L. R. (2012). Connecting Canadians?: Community Informatics Perspectives on Community Networking Initiatives. In A. Clement, M. Gurstein, G. Longford, A. Moll, & L. R. Shade (Eds.), *Connecting Canadians: Investigations in community informatics* (pp. 3–32). Edmonton: AU Press. Retrieved December 4, 2017, from http://www.aupress.ca/index.php/books/120193

Macaulay, T. (2010). Upstream Intelligence: A New Layer of Cybersecurity. *IAnewsletter*, *13*(3), 22–36.

Macaulay, T. (2015, November). *Risk Management and the Internet of Things*. Presented at the JIQ 2015, Quebec City. Retrieved August 2, 2016, from https://www.youtube.com/watch?v=1H6PnxJ95jM

MacDonald, M. (2014, February 20). Eastlink gets rural broadband deadline. Retrieved January 24, 2015, from http://www.cbc.ca/1.2545211

MacDougall, R. (2013). *The People's Network: The Political Economy of the Telephone in the Gilded Age*. Philadelphia: University of Pennsylvania Press.

MacKinnon, R. (2012). *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

Majone, G. (1997). From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance. *Journal of Public Policy*, *17*(2), 139–167.

Malik, O., & Higginbotham, S. (2013, June 17). Having problems with your Netflix? You can blame Verizon. Retrieved June 19, 2013, from http://gigaom.com/2013/06/17/having-problems-with-your-netflix-you-can-blame-verizon/

Marck, P. (2005, June 29). Public may never know all contract details: Privacy commissioner cites confidentiality. *Edmonton Journal*, p. G3.

Marck, P. (2007, June 22). Telus bids to acquire Bell and rule Canada telecom; Bell's business has not grown as predicted; ambitious competitor looks to cash in. *Edmonton Journal*, p. E7.

Marlow, I. (2010, November 15). Rural Canada loses as politics and business fail to get broadband down the last mile. Retrieved December 4, 2017, from http://www.theglobeandmail.com/news/national/time-to-lead/rural-canada-loses-as-politics-and-business-fail-to-get-broadband-down-the-last-mile/article1315241/

Marlow, I., & McNish, J. (2010, April 3). Canada's digital divide. Retrieved December 4, 2017, from http://www.theglobeandmail.com/technology/canadas-digital-divide/article1372555/

Marowits, R. (2007, June 21). Telus considers Bell merger. Retrieved May 25, 2016, from https://www.thestar.com/business/2007/06/21/telus_considers_bell_merger.html

Martin, M. (1991). *Hello, Central?: Gender, Technology, and Culture in the Formation of Telephone Systems*.

Montreal: McGill-Queen's Press.

Massot, E. (2011, June 22). Internet provider cries foul over gas co-op. Retrieved November 27, 2017, from http://www.cochranetimes.com/2011/06/22/internet-provider-cries-foul-over-gas-co-op

Maurer, T. (2012, September 10). Breaking Bad: How America's biggest corporations became cyber vigilantes. *Foreign Policy*. Retrieved December 4, 2017, from http://www.foreignpolicy.com/articles/2012/09/10/breaking_bad

May, C. (2010). *The Global Political Economy of Intellectual Property Rights: The New Enclosures* (2nd ed.). New York: Routledge.

May, C., & Sell, S. K. (2006). *Intellectual Property Rights: A Critical History*. Boulder: Lynne Rienners Publishers.

McKenna, A. (2011, November 28). Téléchargement de The Hurt Locker: des internautes canadiens poursuivis. Retrieved February 26, 2014, from http://techno.lapresse.ca/nouvelles/internet/201111/28/01-4472247-telechargement-de-the-hurt-locker-des-internautes-canadiens-poursuivis.php

McMahon, D. (2011). *The Canadian Cyber Security Situation in 2011*. Retrieved from https://citizenlab.org/cybernorms2012/cybersecurityfindings.pdf

McMahon, D., & Macaulay, T. (2010). Upstream Intelligence in the World of Legal Compliance and Liability. *IAnewsletter*, *13*(4), 24–27.

McMahon, R. (2013, May 31). *Digital self-determination: Aboriginal peoples and the network society in Canada* (dissertation). Simon Fraser University. Retrieved December 4, 2017, from http://summit.sfu.ca/item/13532

McMahon, R., Gurstein, M., Beaton, B., O'Donnell, S., & Whiteduck, T. (2014). Making Information Technologies Work at the End of the Road. *Journal of Information Policy*, *4*(0).

McManus, T. (2015, February 5). New West embarks on fibre-optic broadband network initiative. Retrieved July 16, 2015, from http://www.newwestrecord.ca/news/new-west-embarks-on-fibre-optic-broadband-network-initiative-1.1754163

McTaggart, C. (2006). Was the Internet Ever Neutral? Presented at the 34th Research Conference on Communication, Information and Internet Policy, Arlington, Virginia. Retrieved December 4, 2017, from http://papers.ssrn.com/abstract=2117601

Mediacaster. (2011, September 9). Canadian ISPs to Deliver Customer Information in Hurt Locker Lawsuit. Retrieved December 4, 2017, from https://web.archive.org/web/20111103084359/http://www.mediacastermagazine.com/news/canadian-isps-to-deliver-customer-information-in-hurt-locker-lawsuit/1000575650/

MediaSmarts. (n.d.). What We Do. Retrieved November 23, 2015, from http://mediasmarts.ca/about-us/what-we-do

Melody, W. H., & Møller, D. (2001). Rights of Way as a Foundation for Infrastructure Competition. In W. H. Melody (Ed.), *Telecom Reform: Principles, Politics and Regulatory Practices* (pp. 119–130). Lyngby: Den Private Ingeniørfond, Technical University of Denmark. Retrieved December 4, 2017, from http://lirne.net/resources/tr/telecomreform.pdf

Menard, F. D., & Denton, T. (1999). Third party access to cable modems in Canada. Retrieved December 4, 2017, from http://tmdenton.com/images/articles/thirdparty_access.pdf

Menzies, P. (2013, September 23). Speech by Peter Menzies, to the annual conference of the Canadian Cable Systems Alliance, Mont-Tremblant, Québec, September 23, 2013. Retrieved August 2, 2015, from http://www.crtc.gc.ca/eng/com200/2013/s130923.htm

Meyer, D. (2015, January 29). Canada cracks down on zero-rating in two net neutrality rulings. Retrieved August 28, 2016, from https://gigaom.com/2015/01/29/canada-cracks-down-on-zero-rating-in-two-net-neutrality-rulings/

Middleton, C. (2011). Structural and Functional Separation in Broadband Networks: An Insufficient Remedy to Competitive Woes in the Candian Broadband Market. In M. Moll & L. R. Shade (Eds.), *The Internet Tree: The State of Telecom Policy in Canada 3.0* (pp. 61–72). Ottawa: Canadian Centre for Policy Alternatives. Retrieved December 4, 2017, from http://www.policyalternatives.ca/sites/default/files/uploads/publications/National%20Office/2011/06/Internet_Tree_0.pdf

Miller, C. C. (2014, March 21). Revelations of N.S.A. Spying Cost U.S. Tech Companies. *The New York Times*. Retrieved December 4, 2017, from http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html

Milleron, J.-C. (1972). Theory of value with public goods: A survey article. *Journal of Economic Theory*, *5*(3), 419–477.

Ministry of Northern Development and Mines. (2010, November 19). Government Partners For New Fibre Optics network in Northern Ontario Communities. Retrieved December 4, 2017, from http://news.ontario.ca/mndmf/en/2010/11/government-partners-for-new-fibre-optics-network-in-northern-ontario-communities.html

Mirani, L. (2015, February 9). Millions of Facebook users have no idea they're using the internet. Retrieved December 4, 2017, from http://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/

Mitchell, C. (2014, January 7). *Justifying a Network with Indirect Cost Savings*. Retrieved December 4, 2017, from http://www.muninetworks.org/content/justifying-network-indirect-cost-savings-community-broadband-bits-episode-80

Mitchell, D. (2007). Broadband at the Margins: Challenges to Supernet Deployment in Rural and Remote Albertan Communities. In D. Taras, M. Bakardjieva, & F. Pannekoek (Eds.), *How Canadians Communicate II: Media, Globalization, and Identity* (p. 261). Calgary: University of Calgary Press.

Mitra, A., & Watts, E. (2002). Theorizing Cyberspace: the Idea of Voice Applied to the Internet Discourse. *New Media & Society*, *4*(4), 479–498.

Moglen, E. (2012, May). *Freedom to Connect 2012 Keynote: "Innovation under Austerity."* Washington DC. Retrieved December 4, 2017, from https://www.softwarefreedom.org/events/2012/freedom-to-connect_moglen-keynote-2012.html

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*.

Monsebraaten, L. (2013, June 3). Rogers Communications offering $9.99 monthly internet to those in Toronto public housing. *The Toronto Star*. Retrieved December 4, 2017, from http://www.thestar.com/news/gta/2013/06/03/rogers_communications_offering_999_monthly_internet_to_those_in_toronto_public_housing.html

Morin, S. (2011). Updated: Business Disclosure of personal information to law enforcement agencies: PIPEDA and the CNA letter of request protocol. *Privacy Pages*. Retrieved December 4, 2017, from https://web.archive.org/web/20130610071851/http://www.cba.org/cba/newsletters-sections/pdf/2011-11-privacy1.pdf

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.

Mosco, V. (2004). *The Digital Sublime: Myth, Power, and Cyberspace*. Cambridge, MA: MIT Press.

Mosco, V. (2009). *The Political Economy of Communication* (2nd ed.). Los Angeles: SAGE.

Mueller, M. L. (2004). *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press.

Mueller, M. L. (2012). Property and Commons in Internet Governance. In E. Brousseau, M. Marzouki, & C. Méadel (Eds.), *Governance, Regulation and Powers on the Internet* (pp. 39–62). Cambridge, U.K.: Cambridge University Press.

Murray, A. D. (2007). *The Regulation of Cyberspace: Control in the Online Environment*. London: Routledge.

Mussio, L. (2001). *Telecom Nation: Telecommunications, Computers, and Governments in Canada*. Montreal: McGill-Queen’s University Press.

National Assembly of Québec. (1918, January 30). 14th Legislature, 2nd Session. Retrieved August 29, 2015, from http://www.assnat.qc.ca/en/travaux-parlementaires/assemblee-nationale/14-2/journal-debats/19180130/91443.html

National Broadband Task Force. (2001). *The New National Dream: Networking the Nation for Broadband Access*. Retrieved December 4, 2017, from http://publications.gc.ca/collections/Collection/C2-574-2001E.pdf

National Capital FreeNet. (2014, October 7). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=National_Capital_FreeNet&oldid=609370122

NCF. (n.d.-a). Canadian Community Networks Conference, 1994. Retrieved April 14, 2015, from http://www.ncf.ca/ncf/freeport2html/conferences/com-net94/menu.html

NCF. (n.d.-b). International Freenet Conference. Retrieved April 14, 2015, from http://www.ncf.ca/ncf/freeport2html/conferences/com-net93/menu.html

Neocleous, M. (2000). Against security. *Radical Philosophy*, (100), 7–15.

Neocleous, M. (2008). *Critique of Security*. Edinburgh: Edinburgh University Press.

Nevis Consulting Group. (2003, August 6). Summary of Submissions to the Lawful Access Consultation. Retrieved October 26, 2015, from http://canada.justice.gc.ca/eng/cons/la-al/sum-res/index.html

Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology*, *7*(2), 61–73.

Noam, E. M. (1994). Beyond liberalization II: The impending doom of common carriage. *Telecommunications Policy*, *18*(6), 435–452.

Norton, W. B. (2011). Internet Service Providers and Peering. Retrieved July 25, 2012, from http://drpeering.net/white-papers/Internet-Service-Providers-And-Peering.html

Nottingham, M. (2014, December 27). Why Intermediation is Important. Retrieved February 1, 2015, from https://www.mnot.net/blog/2014/12/27/why_intermediation_is_important

Nowak, P. (2009, August 12). Bell and Telus will merge within 2 years, RBC predicts. Retrieved May 25, 2016, from http://www.cbc.ca/news/technology/bell-and-telus-will-merge-within-2-years-rbc-predicts-1.787085

Nowak, P. (2010, August 31). Bell, Telus must rebate phone customers: CRTC. Retrieved April 25, 2015, from http://www.cbc.ca/1.876114

NSA. (2009). *ST-09-0002 Working Draft*. Retrieved December 4, 2017, from http://www.guardian.co.uk/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection

NSA. (2013, April 3). NSA Intelligence Relationship with Canada's Communications Security Establishment Canada (CSEC). Retrieved December 4, 2017, from https://www.aclu.org/sites/default/files/assets/2013.12.10_nsa_csec_partnership.pdf

O'Brien, G. (2013, February 14). Independent ISP Distributel fighting moviemakers over customer privacy. Retrieved February 20, 2013, from http://www.cartt.ca/news/15099/Cable-Telecom/Independent-ISP-Distributel-fighting-moviemakers-over-customer-privacy.html

OECD. (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved November 4, 2015, from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD. (2011). *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. OECD Publishing. Retrieved December 4, 2017, from http://www.oecd.org/sti/interneteconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm

OECD. (2012). *Report on Experiences with Structural Separation*. OECD. Retrieved December 4, 2017, from http://www.oecd.org/daf/competition/50056685.pdf

Office of the Auditor General of Canada. (2012). *Report of the Auditor General of Canada to the House of Commons*. Ottawa: Office of the Auditor General of Canada. Retrieved December 4, 2017, from http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html

Office of the Privacy Commissioner. (2014, October 30). Metadata and Privacy - A Technical and Legal Overview. Retrieved December 4, 2017, from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/

Office of the Privacy Commissioner. (2015a). *Any and all records including but not limited to memos, written notes, presentations, emails, reports & correspondence prepared for or by Privacy Commissioner Daniel Therrien concerning the OPC's investigation into the RCMP's use of warrantless requests for Canadians' personal information and the OPC's subsequent report on same from August 1, 2014 to November 1, 2014* (ATI Request No. A-2014-00158). Retrieved December 4, 2017, from http://paroxysms.ca/csis_random/csis_cyberwar.pdf

Office of the Privacy Commissioner. (2015b, April 7). Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program. Retrieved December 4, 2017, from https://www.priv.gc.ca/cf-dc/2015/2015_001_0407_e.asp

Office of the Privacy Commissioner. (2015c, June 30). Transparency Reporting by Private Sector Companies: Comparative Analysis. Retrieved December 4, 2017, from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2015/transp_201506/

OICRD. (2011). *Finishing the Dream: Final Project Report, Olds Extended Community Engagement Site*. Retrieved December 4, 2017, from http://www.oldscc.com/Olds_Extended_CES_Final_Report_to_RADF_letter.pdf

OICRD. (2013). *Technology Committee 2012-2013 Annual Report*. Retrieved December 16, 2013, from http://www.oldsinstitute.ca/pdfs/agm13tek.pdf

OICRD. (2015). Annual General Meeting & Report to the Community. Retrieved December 4, 2017, from http://www.oldsinstitute.com/wp-content/uploads/2015/07/2015-OI-AGM-Report2.pdf

O'Mahoney, J. (2012). Embracing essentialism: A realist critique of resistance to discursive power. *Organization*, *19*(6), 723–741.

O'Malley, P. (2016). Foreword. In R. K. Lippert, K. Walby, I. Warren, & D. Palmer (Eds.), *National security, surveillance and terror: Canada and Australia in comparative perspective* (pp. v-vii). London: Palgrave Macmillan.

OpenMedia. (2011). Stop The Meter On Your Internet Usage. Retrieved April 10, 2016, from https://web.archive.org/web/20110217051644/http://www.stopthemeter.ca/

OpenMedia. (2015, February 2). Telecom Notice of Consultation CRTC 2013-551, Review of wholesale services and associated policies: Reply to Cost Claims. Retrieved from https://services.crtc.gc.ca/pub/DocWebBroker/OpenDocument.aspx?Key=108871&Type=Notice

Pacienza, A. (2004, February 16). Cdn recording industry begins legal fight to stop music uploaders. *Canadian Press*.

Pai, A. (2017, June 7). FCC Chairman Pai addresses The 2017 Canadian Telecom Summit. Retrieved June 7, 2017, from http://mhgoldberg.com/blog/?p=11380

Palmer, P. (2015, March 18). Structural Separation: It's Time to be Impolite. Retrieved March 14, 2016, from http://philippalmerlaw.ca/structural-separation-its-time-to-be-impolite/

Paltridge, S. (1995). *Telecommunication infrastructure: The benefits of competition*. Paris: Organisation for Economic Co-operation and Development.

Paperny, A. M. (2012, June 29). Telcos in talks with Ottawa to shape Internet "spy" bill: documents. Retrieved December 4, 2017, from http://www.theglobeandmail.com/technology/tech-news/telcos-in-talks-with-ottawa-to-shape-internet-spy-bill-documents/article4376958/

Parsons, C. (2011, November 21). The Anatomy of Lawful Access Phone Records. Retrieved November 2, 2015, from https://www.christopher-parsons.com/the-anatomy-of-lawful-access-phone-records/

Parsons, C. (2012, February 28). The Issues Surrounding Subscriber Information in Bill C-30. Retrieved November 1, 2015, from https://www.christopher-parsons.com/the-issues-surrounding-subscriber-information-in-bill-c-30/

Parsons, C. (2013). *The Politics of Deep Packet Inspection: What Drives Surveillance by Internet Service Providers?* (dissertation). University of Victoria.

Parsons, C. (2015a). Stuck on the Agenda: Drawing Lessons from the Stagnation of "Lawful Access" Legislation in Canada. In M. Geist (Ed.), *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (pp. 257–283). Ottawa: University of Ottawa Press. Retrieved December 4, 2017, from http://www.ruor.uottawa.ca/bitstream/10393/32424/1/9780776621838_WEB.pdf

Parsons, C. (2015b). *The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians*. Telecom Transparency Project. Retrieved December 4, 2017, from http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf

Parsons, C. (2017). The (In)effectiveness of Voluntarily Produced Transparency Reports. *Business & Society*.

Paterson, N. (2012). Walled Gardens: The New Shape of the Public Internet. In *Proceedings of the 2012 iConference* (pp. 97–104). New York: ACM.

Payton, L. (2014). *Online privacy decision means "back to the drawing board" for Tories*. Retrieved December 4, 2017, from http://www.cbc.ca/1.2674793

Pedersen, J. S., & Dobbin, F. (1997). The social invention of collective actors on the rise of the organization. *American Behavioral Scientist*, *40*(4), 431–443.

Perlroth, N., Larson, J., & Shane, S. (2013, September 5). N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *The New York Times*. Retrieved December 4, 2017, from http://www.nytimes.com/2013/09/06/us/nsa-foils-much-inter net-encryption.html

Pitts, G. (2012, January 22). Canada needs to reinvent CRTC, outgoing head says. Retrieved December 14, 2015, from http://www.theglobeandmail.com/report-on-business/canada-needs-to-reinvent-crtc-outgoing-head-says/article554489/

Porpora, D. V. (2016). *Reconstructing Sociology: The Critical Realist Approach*. Cambridge U.K.: Cambridge University Press.

Power, E. M. (2013). *The Law of Privacy*. Markham: LexisNexis.

Public Safety Canada. (2011a, October 22). Canada's Cyber Security Strategy. Retrieved December 4, 2017, from http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

Public Safety Canada. (2011b, October 22). Summary of public consultation on access to customer name and address information for public safety purposes. Retrieved December 4, 2017, from https://web.archive.org/web/20130731190554/http://www.publicsafety.gc.ca/prg/ns/sum-conslt-eng.aspx

Public Safety Canada. (2012a). *2011 incident reports and ministerial briefings concerning cyber attacks, as well as the budgets for CCIRC from 2010-2012 and projected costs for the upcoming year* (ATI Request No. A-2011-00253).

Public Safety Canada. (2012b). *All records from March 1 to November 4, 2011 about Canada's privacy commissioners' positions on the proposed lawful access bills* (ATI Request No. A-2011-00220).

Public Safety Canada. (2012c). *Records from November 1, 2011 to February 10, 2012 regarding the hacker group Anonymous* (ATI Request No. A-2011-00318).

Public Safety Canada. (2012d). *Records on Government consultations with law enforcement and justice officials concerning the negative impact of a warrant requirement for basic subscriber information* (ATI Request No. A-2011-00255). Retrieved December 4, 2017, from http://telecomtransparency.org/wp-content/uploads/2015/07/A-2011-00255.pdf

Public Safety Canada. (2013a). *All briefing material from the ADM level and above re: cyber security capabilities in government of Canada systems from January 1 2010 to October 22 2012* (ATI Request No. A-2012-00264[1]).

Public Safety Canada. (2013b). *Correspondence from the public on Bill C-30 from Feb 1 May 10, 2012* (ATI Request No. A-2012-00301).

Public Safety Canada. (2013c). *Lawful Interception of Telecommunications* (ATI Request No. A-2012-00457).

Public Safety Canada. (2013d). Public Safety ATIP: Telecom Equipment. Retrieved July 26, 2016, from https://www.scribd.com/document/250135436/Public-Safety-ATIP-Telecom-Equipment

Public Safety Canada. (2013e). *Records concerning Bill C-30 currently before Parliament, from Oct 1 to Dec 3, 2012* (ATI Request No. A-2012-00333).

Public Safety Canada. (2013f). *Records on requests made by law enforcement agencies to ISPs or online entities to gain access to Internet users' personal information from January 1, 2011 to July 11, 2012* (ATI Request No. A-2012-00113).

Public Safety Canada. (2013g). *Records on the government's Cyber Security Strategy dated from July 1, 2011 to April 27, 2012* (ATI Request No. A-2012-00016).

Public Safety Canada. (2014a). *Hacker group Anonymous - especially on '#OPPartyCrasher', from January 2012 to May 9, 2013* (ATI Request No. A-2013-00070).

Public Safety Canada. (2014b). *Lawful access legislation produced between Jan 1, 2012 and July 31, 2012* (ATI Request No. A-2013-00234).

Public Safety Canada. (2014c). *Records created and/or gathered from January 1, 2013 to May 1, 2014 concerning leaks of American security documents by Edward Snowden, as well as Public Safety Canada's internal response* (ATI Request No. A-2014-00039).

Public Safety Canada. (2014d, March 4). Public Safety Canada Quarterly Financial Report for the Quarter Ended June 30, 2013. Retrieved December 4, 2017, from http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/qrtrl-fnncl-rprt-20130630/index-eng.aspx

Public Safety Canada. (2015a). *PS-000483, September 26, 2014 (Issuing guidance to telecommunication service providers on transparency reporting)* (ATI Request No. A-2014-00299).

Public Safety Canada. (2015b). *Records on internet exchange point 151 Front Street, also known as TORIX, and/or property owner Allied properties REIT* (ATI Request No. A-2014-00059).

Public Safety Canada. (2016). *Presentations re: National Cyber Security Directorate under file PS NCSB 07 (January 1, 2014 to July 3, 2015)* (ATI Request No. A-2015-00103).

Pyburne, P., & Jolly, R. (2014, August 8). Australian Governments and dilemmas in filtering the Internet: juggling freedoms against potential for harm. Retrieved August 19, 2016, from http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1415/InternetFiltering#_Toc395250021

R. v Rogers Communications (2016). ONSC 70**.** Retrieved December 4, 2017, from http://canlii.ca/t/gmx3q

R. v. Spencer (2014). 2 SCR 212. Retrieved December 4, 2017, from http://scc-csc.lexum.com/scc-csc/scc-csc/en/14233/1/document.do

R. v. TELUS (2013). 2 SCR 3. Retrieved December 4, 2017, from http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/12936/index.do

Rabideau, M. (1991). Duarte v. R.: In Fear of Big Brother. *University of Toronto Faculty of Law Review*, *49*, 171–185.

Rahamim, Y. (2004). Wiretapping and Electronic Surveillance in Canada: The Present State of the Law and Challenges to the Employment of Sophisticated and Intrusive Technology in Law Enforcement. *Windsor Review of Legal and Social Issues*, *18*, 87–104.

Rajabiun, R., & Middleton, C. (2013). Rural Broadband Development in Canada's Provinces: An Overview of Policy Approaches. *Journal of Rural and Community Development*, *8*(2), 7–22.

Rajabiun, R., & Middleton, C. (2015). Public Interest in the Regulation of Competition. *Journal of Information Policy*, *5*, 32–66.

RCMP bypassed Bell, pried open terminal box to tap apartment phone. (1977, February 19). *Globe and Mail*, p. 1.

Reed, D. P. (2010, December 15). A response to Barbara van Schewick: code needs (only a little) help from the law. Retrieved December 4, 2017, from http://www.reed.com/blog-dpr/?p=85

Reed, D. P. (2013, September 26). What The Internet Is, and Should Continue To Be. Retrieved December 4, 2017, from http://www.reed.com/blog-dpr/?p=132

Rens, J.-G. (2001). *The invisible empire a history of the telecommunications industry in Canada*. (K. Roth, Trans.).

Montreal, Que.: McGill-Queen's University Press. Retrieved from http://site.ebrary.com/id/10121254

Reo, J. (2016, August 11). Customers Want "Clean Pipe." Retrieved December 4, 2017, from http://www.corero.com/blog/750-customers-want-clean-pipe.html

Richard, M., & Philpot, D. (2013). GoFred: Municipally-Owned ICT Utilities in Fredericton, New Brunswick. *The Journal of Community Informatics*, *10*(2). Retrieved December 4, 2017, from http://ci-journal.net/index.php/ciej/article/view/993

Rideout, V. (2003). *Continentalizing Canadian Telecommunications: The Politics of Regulatory Reform*. Montreal: McGill-Queen's University Press.

Rideout, V., & Reddick, A. J. (2005). Sustaining Community Access to Technology: Who Should Pay and Why. *The Journal of Community Informatics*, *1*(2). Retrieved December 4, 2017, from http://ci-journal.net/index.php/ciej/article/view/202

Roberts, D., & Kiss, J. (2013, December 9). Twitter, Facebook and more demand sweeping changes to US surveillance. *The Guardian*. Retrieved December 4, 2017, from http://www.theguardian.com/world/2013/dec/09/nsa-surveillance-tech-companies-demand-sweeping-changes-to-us-laws

Roberts, P. (2011, November 17). Answering your most-asked questions about Axia's new Internet Gateway Service. Retrieved October 19, 2013, from http://albertasupernetblog.thealbertasupernet.com/?p=825

Rogers. (2004, March 12). Written Representations of Rogers Communications Inc. Retrieved December 11, 2015, from https://cippic.ca/sites/default/files/file-sharing-lawsuits/Rogers_Written_Reps_Mar12.pdf

Rogers. (2014). 2013 Transparency Report. Retrieved June 7, 2014, from http://www.rogers.com/cms/images/en/S35635%20Rogers-2013-Transparency-Report-EN.pdf

Rogers. (2016). 2015 Transparency Report. Retrieved May 20, 2016, from http://about.rogers.com/about/helping-our-customers/transparency-report

RogersKevin. (2016, May 19). More transparency about how we protect your privacy when asked for your info. Retrieved May 20, 2016, from http://redboard.rogers.com/2016/05/19/more-transparency-about-how-we-protect-your-privacy-when-asked-for-your-info/

Romaniuk, B. S., & Janisch, H. N. (1986). Competition in Telecommunications: Who Polices the Transition. *Ottawa Law Review*, *18*(3), 561–661.

Roseman, E. (2012, January 24). Stop throttling video games, CRTC tells Rogers. Retrieved May 14, 2016, from https://www.thestar.com/business/personal_finance/spending_saving/2012/01/24/stop_throttling_video_games_crtc_tells_rogers.html

Rossland Broadband Initiative. (n.d.). Benefits. Retrieved July 24, 2015, from http://www.rosslandbroadband.com/benefits.html

Rubinstein, D. (2001, April 26). Vision key to landing mega Supernet project. *Edmonton Journal*, p. H14.

Rushe, D. (2014, August 30). Chattanooga's Gig: how one city's super-fast internet is driving a tech boom. Retrieved January 29, 2015, from http://www.theguardian.com/world/2014/aug/30/chattanooga-gig-high-speed-internet-tech-boom

Rushe, D., & Lewis, P. (2013, December 17). Tech firms push back against White House efforts to divert NSA meeting. *The Guardian*. Retrieved December 4, 2017, from http://www.theguardian.com/world/2013/dec/17/tech-firms-obama-meeting-nsa-surveillance

Sandvine. (2013). *Exposing the Technical and Commercial Factors Underlying Internet Quality of Experience*. Retrieved December 4, 2017, from https://www.sandvine.com/downloads/general/global-internet-phenomena/2013/exposing-the-technical-and-commercial-factors-underlying-internet-quality-of-experience.pdf

Sandvine. (2016). Cyber Security Considerations and Techniques. Retrieved August 2, 2016, from https://www.sandvine.com/downloads/general/whitepapers/cyber-security-considerations-and-techniques.pdf

Sangster, J. (1978). The 1907 Bell Telephone Strike: Organizing Women Workers. *Labour/Le Travail*, *3*, 109–130.

Sargsyan, T. (2016). Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security. *International Journal of Communication*, *10*, 2221–2237.

SaskTel. (2014). SaskTel 2013 Transparency Report. Retrieved December 4, 2017, from https://www.scribd.com/doc/241607582/SaskTel-2013-Transparency-Report

Sayer, A. (2000). *Realism and Social Science*. London: SAGE.

Sayer, P. (2015, October 7). Verizon will use its mobile supercookie to target customers with AOL ads. Retrieved February 9, 2016, from http://www.pcworld.com/article/2990094/privacy/verizon-will-use-its-mobile-supercookie-to-target-customers-with-aol-ads.html

Scalet, S. D. (2007, July 12). Pipe Cleaners: Telcos Offer Managed Security Services. Retrieved August 2, 2016, from http://www.csoonline.com/article/2121659/malware-cybercrime/pipe-cleaners--telcos-offer-managed-security-services.html

SOCAN v. CAIP (2004). 2 SCR 427. Retrieved December 4, 2017, from http://www.canlii.org/en/ca/scc/doc/2004/2004scc45/2004scc45.html

Schneier, B. (2012, November 26). When It Comes to Security, We're Back to Feudalism. Retrieved December 4, 2017, from http://www.schneier.com/essay-406.html

Schnurr, J. (2016, December 21). Low cost internet for Ottawa Community Housing tenants. Retrieved December 30, 2016, from http://ottawa.ctvnews.ca/low-cost-internet-for-ottawa-community-housing-tenants-1.3213142

Schultz, R. J. (1999). Still Standing: The CRTC, 1976-1996. In G. B. Doern, M. M. Hill, M. J. Prince, & R. J. Schultz (Eds.), *Changing the rules: Canadian regulatory regimes and institutions* (pp. 29–56). Toronto: University of Toronto Press.

Scott, P. (2001, September 29). Free-Net Access Points. Retrieved April 11, 2015, from https://web.archive.org/web/20010929112249/http://www.lights.ca/freenet/

Scott, W. R. (2004). Reflections on a Half-Century of Organizational Sociology. *Annual Review of Sociology*, *30*(1), 1–21.

Scotton, G. (2001, September 15). SuperNet costs add to Axia loss. *Calgary Herald*, p. E11.

Selwyn, N. (2004). Reconsidering Political and Popular Understandings of the Digital Divide. *New Media & Society*, *6*(3), 341–362.

Semenova, A., & Wagner, W. J. (2014). Legislative developments — privacy rights in the digital age. Retrieved February 3, 2016, from https://www.gowlings.com/KnowledgeCentre/article.asp?pubID=3814

Sepulvado, J. (2014, January 22). Rural Canadian Town Offers 'Google-Fast' Broadband Service. Retrieved December 4, 2017, from http://www.govtech.com/network/Rural-Canadian-Town-Offers-Google-Fast-Broadband-Service.html?elq=a3d3ce8ff1014680a9164f8ba0f3d3ee&elqCampaignId=6280

Servon, L. J. (2002). *Bridging the Digital Divide: Technology, Community and Public Policy*. Malden: Blackwell.

Settles, C. (2012, October). O Canada, Land of Community Broadband? *Broadband Communities*. Retrieved December 4, 2017, from http://bbcmag.epubxp.com/i/90470/79

Shade, L. R. (1994). Computer Networking in Canada: From CA*net to CANARIE. *Canadian Journal of Communication*, *19*(1). Retrieved December 4, 2017, from http://www.cjc-online.ca/index.php/journal/article/view/794

Shaffer, G. (2011). Peering Ahead: An Examination of Peer-to-Peer Signal-Sharing Communities that Create Their Own Affordable Internet Access. *Canadian Journal of Communication*, *36*(1). Retrieved December 4, 2017, from http://www.cjc-online.ca/index.php/journal/article/view/2314

Shaw. (2004, March 10). Written Representations of Shaw Communications Inc. Retrieved December 11, 2015, from https://cippic.ca/sites/default/files/file-sharing-lawsuits/FurtherWrittenSubmissionsShaw.pdf

Shaw, E., & Valiquet, D. (2012, February 15). Legislative Summary of Bill C-30: An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts. Retrieved October 26, 2015, from http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/41/1/c30-e.pdf

Shaw, G. (2004, April 1). Sharing music over Internet not illegal, Federal Court rules. *The Vancouver Sun*, p. A1.

Shaw, R. (2012, March 14). Competitors slam "unfair" government deal with Telus; Companies call 10-year contract flawed, suggesting taxpayers will not get the best value for money as a result. *The Vancouver Sun*, p. A6.

Shearing, C., & Johnston, L. (2010). Nodal Wars and Network Fallacies: A Genealogical Analysis of Global Insecurities. *Theoretical Criminology*, *14*(4), 495–514.

Silva, M., & Cartwright, G. F. (1992). The Canadian Network for the Advancement of Research, Industry, and Education (CANARIE). *Public Access-Computer Systems Review*, *3*(6). Retrieved December 4, 2017, from https://journals-tdl-org.login.ezproxy.library.ualberta.ca/pacsr/index.php/pacsr/article/view/6068

Singer, L. (2012, July). Unwarranted access? *National*. Retrieved December 4, 2017, from http://www.nationalmagazine.ca/Articles/June-2012-Issue/Unwarranted-access.aspx

Singer, M. G. (1965). Negative and Positive Duties. *The Philosophical Quarterly*, *15*(59), 97–103.

Smith, G. J. H. (2007). *Internet Law and Regulation*. London: Sweet & Maxwell.

Solomon, H. (2011, November 16). Surveillance law could close small ISPs: Lawyer. Retrieved December 4, 2017, from http://www.itworldcanada.com/news/surveillance-law-could-close-small-isps-lawyer/144316

Solomon, H. (2016a, December 6). Protect privacy of subscribers, but don't stick us with the bill, CWTA tells Ottawa. Retrieved December 23, 2016, from https://cartt.ca/article/protect-privacy-subscribers-don%E2%80%99t-stick-us-bill-cwta-tells-ottawa

Solomon, H. (2016b, December 21). Police have enough power, court orders still required, network owners tell Ottawa. Retrieved December 23, 2016, from https://cartt.ca/article/police-have-enough-power-court-orders-still-required-network-owners-tell-ottawa

sssscary. (2012, December 11). IP logging retention. *DSLReports Forums: Start Communications*. Retrieved February 28, 2014, from http://www.dslreports.com/forum/r27809164-IP-logging-retention

Standing Committee on Industry, Science and Technology. (2006, November 7). Standing Committee on Industry, Science and Technology - Evidence: Tuesday November 7, 2006. Retrieved December 4, 2017, from http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=2485667&Language=E&Mode=1

Standing Senate Committee on Legal and Constitutional Affairs. (2009, May 14). Proceedings: Issue 8 - Evidence for May 14, 2009. Retrieved December 4, 2017, from http://www.parl.gc.ca/Content/SEN/Committee/402/lega/08evb-e.htm?Language=E&Parl=40&Ses=2&comm_id=11

Standing Senate Committee on National Security and Defence. (2012, May 7). Proceedings: Issue 6, Evidence - Meeting of May 7, 2012. December 4, 2017, from http://www.parl.gc.ca/content/sen/committee/411/SECD/06EVB-49519-E.HTM

Stevens, G. (1976, August 6). The "consumer's empty chair." *Globe and Mail*, p. 6.

Stoddart, J., Work, F., Denham, E., Hamilton, I., Bertrand, A. E., Ring, E., … McPhee, T.-A. (2011, March 9). Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the current "Lawful Access" proposals. Retrieved February 18, 2016, from https://www.priv.gc.ca/media/nr-c/2011/let_110309_e.asp

Stoesser, J. (2015, February 11). Council looking into fibre optic network. Retrieved March 27, 2015, from http://www.pinchercreekecho.com/2015/02/11/council-looking-into-8-million-fibre-optic-network

Stone, A. (1991). *Public Service Liberalism: Telecommunications and Transitions in Public Policy*. Princeton: Princeton University Press.

Stryker, S. (1980). *Symbolic interactionism: A social structural version*. Menlo Park: Benjamin-Cummings Publishing Company.

Sturgeon, J. (2012, June 12). Telus and Bell's wireless partnership still a sore spot for competitors. Retrieved November 18, 2013, from http://business.financialpost.com/2012/06/12/telus-and-bells-wireless-partnership-still-a-sore-spot-for-competitors/

SWIFT. (2016, July 26). SWIFT receives $180 million in provincial and federal finding through Small Communities

Fund. Retrieved September 26, 2016, from http://swiftnetwork.ca/SWIFT_Media_Release_July_26_2016.pdf

Szarycz, G. S. (2010). Challenges and opportunities in elite social science research: Interviewing top executives in tourism-business contexts. In G. S. Szarycz (Ed.), *Research Realities in the Social Sciences: Negotiating Fieldwork Dilemmas* (pp. 151–184). Amherst: Cambria Press.

Taddese, Y. (2016, August 22). Lawyers call for national cybersecurity standards. Retrieved August 31, 2016, from http://www.canadianlawyermag.com/legalfeeds/3404/lawyers-call-for-national-cybersecurity-standards.html

Tapia, A. H., & Ortiz, J. A. (2008a). Keeping Promises: Municipal communities struggle to fulfill promises to narrow the digital divide with Municipal Community Wireless Networks. *The Journal of Community Informatics*, *4*(1). Retrieved December 4, 2017, from http://ci-journal.net.login.ezproxy.library.ualberta.ca/index.php/ciej/article/view/436

Tapia, A. H., & Ortiz, J. A. (2008b). Keeping Promises: Municipal communities struggle to fulfill promises to narrow the digital divide with Municipal Community Wireless Networks. *The Journal of Community Informatics*, *4*(1). Retrieved December 4, 2017, from http://ci-journal.net/index.php/ciej/article/view/436

Taylor, R. P. (1993). The NCF Federal Election Project. Presented at the International Freenet Conference, Ottawa. Retrieved December 4, 2017, from http://www.ncf.ca/ncf/freeport2html/conferences/com-net93/papers/richard_taylor.txt.html

TekSavvy. (2014, June 4). TekSavvy Transparency Report. Retrieved June 7, 2014, from http://teksavvy.com/Media/Default/Citizen%20Lab/TekSavvy%20to%20Citizenlab%20-%202014-06-04.pdf

TekSavvy. (2015, November 5). Transcript Brief. Retrieved December 16, 2015, from https://cippic.ca/sites/default/files/CF_No._T-2058-12_-_TekSavvy_ats_Voltage_-_Transcript_Brief.pdf

TekSavvy. (2016, November 28). Shared Internet Resources Policy. Retrieved January 8, 2017, from https://www.teksavvy.com/en/why-teksavvy/policies/legal-stuff/internet-traffic-management-practices

Telecommunications Policy Review Panel. (2006). Final Report. Retrieved March 3, 2016, from https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/tprp-final-report-2006.pdf/$FILE/tprp-final-report-2006.pdf

Telecommunities Canada, & Industry Canada. (1997, August 17). Framework for Co-Operation between Telecommunities Canada (TC) and Industry Canada to enhance the ability of Canadian communities to utilize electronic public space. Retrieved October 3, 2015, from http://tc.ca/framework.html

TELUS. (2004, March 11). Written Representations. Retrieved December 11, 2015, from https://cippic.ca/sites/default/files/file-sharing-lawsuits/Written_Representations.pdf

TELUS. (2014). TELUS Transparency Report 2013. Retrieved September 19, 2014, from http://about.telus.com/servlet/JiveServlet/downloadBody/5544-102-1-6081/TELUS%20Transparency%20Report%202013%20-English.pdf

TELUS. (2015, January 26). Review of wholesale services and associated policies, Telecom Notice of Consultation

CRTC 2013-551: Answer to Cost Claims. Retrieved December 4, 2017, from https://services.crtc.gc.ca/pub/DocWebBroker/OpenDocument.aspx?Key=108871&Type=Notice

TELUS. (2016a). 2015 TELUS Sustainability Report. Retrieved May 11, 2015, from https://sustainability.telus.com/wordpress/wp-content/uploads/2016/06/2015_Sustainability_Report-EN.pdf

TELUS. (2016b, October 14). TELUS launches Internet for Good pilot to support 18,000 British Columbian families. Retrieved October 15, 2016, from http://about.telus.com/community/english/news_centre/news_releases/blog/2016/10/14/telus-launches-internet-for-good-pilot-to-support-18000-british-columbian-families?CMP=SOC_AMP

TELUS. (n.d.). Telus WISE. Retrieved February 7, 2016, from http://wise.telus.com/

The Guardian. (2015, January 30). Island Telecom taking over internet service in Summerside. Retrieved July 14, 2015, from http://www.theguardian.pe.ca/Business/2015-01-30/article-4026220/Island-Telecom-taking-over-internet-service-in-Summerside/1

The Wire Report. (2011, January 13). CRTC denies Axia request to revise Telus use of deferral funds. Retrieved October 13, 2013, from http://www.thewirereport.ca/briefs/2011/01/13/crtc-denies-axia-request-to-revise-telus-use-of-deferral-funds/21812

Therrien, D. (2015, February 12). Submission to the Standing Committee on Industry, Science and Technology. Retrieved November 15, 2015, from https://www.priv.gc.ca/parl/2015/parl_sub_150212_e.asp

Thies, C. G., & Breuning, M. (2012). Integrating Foreign Policy Analysis and International Relations through Role Theory. *Foreign Policy Analysis*, *8*(1), 1–4.

Thompson, R. (2004, February 14). Shaw won’t breach privacy to nab Net pirates: Music industry taking case to court. *Edmonton Journal*, p. A3.

Timmermans, S., & Epstein, S. (2010). A World of Standards but not a Standard World: Toward a Sociology of Standards and Standardization. *Annual Review of Sociology*, *36*(1), 69–89.

Toews, V. (2012, February 28). House of Commons Debates. Retrieved November 22, 2015, from https://openparliament.ca/debates/2012/2/28/vic-toews-1/

Trichur, R. (2013, July 24). Rogers CEO calls for ‘level playing field’ as Verizon eyes Canada. Retrieved December 4, 2017, from http://www.theglobeandmail.com/report-on-business/rogers-profit-revenue-climb/article13384991/

Trichur, R., Silcoff, S., & Erman, B. (2013, May 18). How Ottawa’s plan to foster wireless competition sank. Retrieved March 16, 2015, from http://www.theglobeandmail.com/report-on-business/how-ottawas-plan-to-foster-wireless-competition-sank/article12005826/

Trilling, S. (2000, October 1). Understanding clean pipe solutions. Retrieved August 7, 2016, from http://enterprisesecurity.symantec.com/article.cfm?articleid=192&PID=349398

Turkle, S. (1994). Constructions and reconstructions of self in virtual reality: Playing in the MUDs. *Mind, Culture, and Activity*, *1*(3), 158–167.

Unland, K. (2000, November 3). Casting the Net over Alberta: Province signs $300M agreement with Bell to extend high-speed Internet access to rural areas. *Edmonton Journal*, p. A1.

Valiquet, D. (2011, February 15). Legislative Summary of Bill C-22: An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service. Retrieved June 22, 2013, from http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?Language=E&ls=c22&Parl=40&Ses=3&source=library_prb

Van der Berg, R. (2008, September 2). How the 'Net works: an introduction to peering and transit. Retrieved December 4, 2017, from http://arstechnica.com/features/2008/09/peering-and-transit/

van Dijk, J. A. G. M. (2006). Digital divide research, achievements and shortcomings. *Poetics*, *34*(4–5), 221–235.

Van Gorp, A., & Middleton, C. A. (2010). The impact of facilities and service-based competition on internet services provision in the Canadian broadband market. *Telematics and Informatics*, *27*(3), 217–230.

van Schewick, B. (2010). *Internet Architecture and Innovation*. Cambridge, MA: The MIT Press.

Vancouver Regional FreeNet Assn. v. M.N.R. (1996). FCR 880. Retrieved December 4, 2017, from http://canlii.ca/t/4ndd

Venugopal, R. (2015). Neoliberalism as concept. *Economy and Society*, *44*(2), 165–187.

Vermette, M.-A., & Iatrou, N. (2010). Norwich Orders in Canada: A Tool for Twenty-First Century Litigation. Retrieved December 4, 2017, from http://www.weirfoulds.com/files/6790_Reprint-NorwichOrders-Original.pdf

Victoria Free-Net Association. (n.d.). About Us. Retrieved April 14, 2015, from http://victoria.tc.ca/about_us.html

Vidéotron. (2004, August 5). Memorandum of Fact and Law of the Third Party Respondent Vidéotron Ltée. Retrieved December 11, 2015, from https://cippic.ca/sites/default/files/file-sharing-lawsuits/videotron_factum.pdf

Vogel, S. K. (1996). *Freer Markets, More Rules: Regulatory Reform in Advanced Industrial Countries*. Ithaca, N.Y.: Cornell University Press.

Voltage Pictures LLC v. John Doe and Jane Doe (2014), FC 161. Retrieved December 4, 2017, from https://www.canlii.org/en/ca/fct/doc/2014/2014fc161/2014fc161.pdf

Voltage Pictures, LLC v. John Doe (2016), FC 881. Retrieved December 4, 2017 from https://www.canlii.org/en/ca/fct/doc/2016/2016fc881/2016fc881.html

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

Walters, W. (2012). *Governmentality: Critical Encounters*. New York: Routledge.

Wark, W. (2016). CSE and Lawful Access After Snowden. Retrieved December 26, 2016, from http://www.cips-cepi.ca/wp-content/uploads/2011/09/WWP-FINALfinal.pdf

Weller, D., & Woodcock, B. (2012). *Internet Traffic Exchange: Market Developments and Policy Challenges* (OECD Digital Economy Papers No. 207). OECD Publishing. Retrieved December 4, 2017, from http://www.oecd-ilibrary.org/science-and-technology/internet-traffic-exchange_5k918gpt130q-en

Wellman, B., & Haythornthwaite, C. (2002). Introduction. In *The Internet in Everyday Life* (pp. 3–41). Malden:

Blackwell.

Wendt, A. (2004). The State as Person in International Theory. *Review of International Studies*, *30*(2), 289–316.

Whalen, C. (2013, September 3). Fibre optic starts going in ground this week. Retrieved December 4, 2017, from http://www.draytonvalleywesternreview.com/2013/09/03/fibre-optic-starts-going-in-ground-this-week

Whitaker, R. (2012). The Curious Tale of The Dog That Hasn't Barked (Yet). *Surveillance & Society*, *10*(3/4), 340–343.

Who we are, what we do, and why you should be a part of it. (2013). Retrieved December 4, 2017, from https://www.youtube.com/watch?v=rrJwPj5wojA

Wiest, P. (2014). Nelson Broadband Project. Retrieved July 25, 2015, from http://futures.bc.ca/wp-content/uploads/2014/05/Nelson-Broadband-Final-Report.pdf

Wilson, K. G. (2000). *Deregulating Telecommunications: U.S. and Canadian Telecommunications, 1840-1997*. Lanham: Rowman & Littlefield.

Wilson, M. (1997, May 15). Awash in choices: 'Net providers rev up rivalry. *The Province*, p. A51.

Wingrove, J. (2014, October 2). Cyberbullying bill C-13 moves on despite Supreme Court decision. Retrieved December 4, 2017, from http://m.theglobeandmail.com/news/politics/cyberbullying-bill-c-13-moves-on-despite-supreme-court-decision/article20885941/

Winseck, D. (1995). A Social History of Canadian Telecommunications. *Canadian Journal of Communication*, *20*(2). Retrieved December 4, 2017, from http://www.cjc-online.ca/index.php/journal/article/view/863

Winseck, D. (1998). *Reconvergence: A Political Economy of Telecommunications in Canada*. Cresskill: Hampton Press.

Winseck, D. (2015a). Intermediary Responsibility. In R. Mansell, P. H. Ang, C. Steinfield, S. van der Graaf, P. Ballon, A. Kerr, … D. J. Grimshaw (Eds.), *International Encyclopedia of Digital Communication and Society* (pp. 488–502). Boston: Wiley-Blackwell. Retrieved December 4, 2017, from http://www.davidellis.ca/wp-content/uploads/2015/01/winseck-Intermediary-Responsibility_Final-APH.pdf

Winseck, D. (2015b, November 10). Media and Internet Concentration in Canada Report, 1984 – 2014. Retrieved November 11, 2015, from http://www.cmcrp.org/2015/11/10/media-and-internet-concentration-in-canada-report-1984-2014/

Winsor, H. (1973, June 18). Wiretap bill: a balance remains elusive. *Globe and Mail*, p. 7.

Wire Report. (2000a, November 6). Bell consortium beats out Telus--Alberta leapfrogs federal gov't in bid to bring broadband to every community. Retrieved October 23, 2013, from http://www.thewirereport.ca/news/2000/11/06/bell-consortium-beats-out-telus--alberta-leapfrogs-federal-gov%E2%80%99t-in-bid-to-bring/15327

Wire Report. (2000b, December 4). Debate over public versus private networks erupts at Canarie conference. Retrieved October 23, 2013, from http://www.thewirereport.ca/news/2000/12/04/debate-over-public-versus-private-networks-erupts-at-canarie-conference/15288

Wire Report. (2004, March 31). Call-Net could be next telco to enter consolidation game with power companies.

Retrieved October 21, 2015, from http://www.thewirereport.ca/news/2004/03/31/call-net-could-be-next-telco-to-enter-consolidation-game-with-power-companies/13256

Wire Report. (2008, November 27). ISPs should take initiative to stop piracy, without the heavy hand of legislation: Quebecor executive. Retrieved November 25, 2013, from http://www.thewirereport.ca/news/2008/11/27/isps-should-take-initiative-to-stop-piracy-without-the-heavy-hand-of-legislation-quebecor/18999

Wolfe, M., Vennard, L., & Mitchell, D. (2014). *Final Report: Alberta Digital Futures Symposium*. Centre for Information & Communication, The Van Horne Institute. Retrieved from http://www.digitalfutures.ca/wp-content/uploads/2013/10/AB-Digital-Futures-Report.pdf

Wood, J. (2006). Research and innovation in the field of security: a nodal governance view. In J. Wood & B. Dupont (Eds.), *Democracy, society and the governance of security* (pp. 217–248). Cambridge, U.K.: Cambridge University Press.

Wood, J., & Shearing, C. D. (2007). *Imagining Security*. Portland, OR: Willan.

Woodhead, T. (2013, August 1). The gift of Verizon. Retrieved December 2, 2015, from http://blog.telus.com/public-policy/the-gift-of-verizon/

Woods, A. (2014, January 9). Canada courting U.S. web giants in wake of NSA spy scandal. *The Toronto Star*. Retrieved from http://www.thestar.com/news/canada/2014/01/09/us_companies_look_to_canadian_servers_in_wake_of_nsa_spy_scandal.html

Woroch, G. A. (1998). Facilities Competition and Local Network Investment: Theory, Evidence and Policy Implications. *Industrial and Corporate Change*, *7*(4), 601–614. https://doi.org/10.1093/icc/7.4.601

Wu, T. (2003). Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law*, *2*, 141–176.

Wyatt, E. (2014, February 3). Fast Internet Is Chattanooga's New Locomotive. *The New York Times*. Retrieved from http://www.nytimes.com/2014/02/04/technology/fast-internet-service-speeds-business-development-in-chattanooga.html

Zajko, M. (2015). Canada's cyber security and the changing threat landscape. *Critical Studies on Security*, *3*(2), 147–161. https://doi.org/10.1080/21624887.2015.1071165

Zajko, M. (2016a). Telecom Responsibilization: Internet Governance, Surveillance, and New Roles for Intermediaries. *Canadian Journal of Communication*, *41*(1), 75–93.

Zajko, M. (2016b, June 29). Watching Six Years of the Regulatory Blockbuster. Retrieved March 29, 2017, from http://zajko.ca/2016/06/29/watching-six-years-of-the-regulatory-blockbuster/

Zezima, K. (2015, July 15). Obama announces pilot program to expand broadband to low-income households. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/post-politics/wp/2015/07/15/obama-to-announce-pilot-program-to-expand-broadband-to-low-income-households/

Zittrain, J. (2003). Internet Points of Control. *Boston College Law Review*, *44*(2), 653–688.

Zittrain, J. (2008). *The future of the internet--and how to stop it*. New Haven, CT: Yale University Press.