Michael Zajko
Assistant Professor, SOCIOLOGY
University of British Columbia
(Okanagan)

Internet Service Providers as Privacy Custodians

Abstract: This article examines the role of internet service providers (ISPs) as guardians of personal information and protectors of privacy, with a particular focus on how telecom companies in Canada have historically negotiated these responsibilities. Communications intermediaries have long been expected to act as privacy custodians by their users, while simultaneously being subject to pressures to collect, utilize, and disclose personal information. 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. Some ISPs have adopted a more positive orientation to this responsibility, actively taking steps to advance it, rather that 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

Introduction

In a digitally-networked society, many of our interactions are carried out through the services of telecommunications companies known as intermediaries, which carry and mediate our communications. This article examines how Canadian internet service providers (ISPs), as a particular class of intermediaries, act as 'privacy custodians' when they govern the privacy of their subscribers and users. ISPs play numerous roles in our society besides simply providing internet access, with each role denoting a position in a social relationship and an associated set of

expectations.[1] In this article I show how the role of privacy custodian has developed in Canadian telecom since the early 2000s, in tension and contradiction with the roles of copyright enforcer, surveillance partner, advertiser, and information merchant. Other scholars (Balkin 2016; Kerr 2002) have argued we could address some of these tensions by seeing intermediaries as fiduciaries and regulating them appropriately. The fiduciary concept has much in common with the role of the privacy custodian, in that it refers to a relationship of dependence between users and ISPs, where an information asymmetry leaves users with little choice but to trust (or hope) that their privacy is being protected by these organization. However, the argument for defining intermediaries as information fiduciaries (Balkin 2016) is a prescriptive one that seeks to align these organizations with a legal category and its obligations; a proposal to address the possibility of harm that these organizations can cause. The concept of privacy custodian refers more broadly to an organization that governs the privacy of its users, whether or not we think this role triggers fiduciary obligations. My interest here is to describe how this role has developed into the present, to identify its tensions and contradictions, and the strategies that ISPs use to navigate these pressures. One of these strategies has been for intermediaries to take a more positive or proactive stance as privacy custodians, voluntarily going beyond statutory obligations. However, privacy custodians exercise discretion both when meeting statutory obligations and when extending their roles further. Intermediaries that take positive steps to strengthen privacy protections and share information about their practices do so selectively, publicizing privacy-enhancing measures while minimizing conduct that users might disapprove of.

Where ISPs have access to vast amounts of sensitive personal information about

[1] On the use of role theory to understand organizations as collective actors, see Abdelnour, Hasselbladh, and Kallinikos 2017.

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. ISPs also act as privacy custodians by limiting the amount of information they collect, even though such collection might be easy or profitable. Privacy custodianship is not just limited to the obligations specified by privacy law, but refers more broadly to how personal information is governed by these organizations. 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.

As privacy custodians, intermediaries must navigate role 'conflicts'[2] when they assist government agencies and other organizations investigating their customers and users (see Kerr & Gilbert 2004). 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. In order for ISPs to operate as agents of surveillance, identification, and targeted marketing, they must reconcile these roles with their conduct as privacy custodians.

Privacy custodians have both positive and negative statutory obligations, and can choose to adopt additional positive responsibilities to protect individual privacy. Canadian ISPs

[2] 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 (Stryker 1980, 73), and has also been used to analyze contradictory roles and expectations of collective or corporate actors in foreign policy analysis and international relations (Thies & Breuning 2012).

are subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which imposes positive responsibilities around accountability, identifying the purposes of collection and obtaining consent, ensuring accuracy of information, and using appropriate safeguards. 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 (schedule 1, cl 4.4-4.5). These negative obligations are recurrently tested by pressures to collect, use and disclose more information, where this serves the needs of government agencies, copyright owners, or corporate profitability. The following table lists the positive and negative statutory responsibilities of ISPs discussed in this article, and the positive responsibilities that some ISPs have been voluntarily adopting.

Table 1

Canadian ISP Responsibilities as Privacy Custodians

Statutory positive responsibilities	Statutory negative responsibilities	Voluntary positive responsibilities
Must be accountable and open about how it governs privacy (PIPEDA, schedule 1, cl 4.1, 4.8, 4.9) Must identify purposes of collection and obtain consent (PIPEDA, schedule 1, cl 4.2-4.3) Must ensure personal information is accurate and properly safeguarded (PIPEDA, schedule 1, cl 4.6-4.7) Must report data breaches	ISP must not collect, use, or disclose personal information without consent unless there are exceptional circumstances (PIPEDA, schedule 1, cl 4.4-4.5; CRTC 2009) ISP must not collect more information than necessary for the purposes consented to (PIPEDA, schedule 1, cl 4.4)	Challenge court orders (Distributel 2013; *R. v. Rogers* [2016]; *R. v. TELUS* [2013]; *BMG Canada Inc. v. John Doe* [2004]) Transparency reports (Parsons 2017) Privacy education (MediaSmarts n.d.) Policy advocacy (Braga 2016; Solomon 2016)

(PIPEDA, s. 10) Must comply with court orders to disclose information or install wiretaps (*Criminal Code*, Part VI ; *Canadian Security Intelligence Service Act*, s. 21; *Competition Act*, s. 11, 15, 16) Must report child pornography (provincial and federal legislation, see Valiquet 2011)		

It is important to note that the above distinction between negative and positive 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 other responsibilities can be difficult to frame in terms of a positive/negative equivalence, and one of the most important 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 (Distributel 2013; *R. v. Rogers* [2016]; *R. v. TELUS* [2013]; *BMG Canada Inc. v. John Doe* [2004]), by interpreting the limitation of disclosure as obliging them to take certain actions in order to protect their users. Effectively, this means that some intermediaries have been adopting more of a positive orientation towards their privacy responsibilities, and playing a more active role in determining what it means to be a privacy custodian. Rather than a legal standard which they 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 the growing recognition of the important role played by privacy custodians, and the efforts of some organizations to differentiate themselves by publicly 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.

Intermediaries, whether these are massive corporate ISPs or not-for-profit community networks, 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, the amount of time these companies choose to retain personal information, how ISPs respond to copyright notices, and in how they share information for reasons of security and law enforcement (Clement and Obar 2016; Kerr 2002; Parsons 2017). 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.

ISPs occupy a strategic position by operating infrastructures that link directly to individual users, providing valuable opportunities for surveillance and identification. Copyright owners, police and security agencies have long recognized this, and attempted to enroll ISPs as active partners in their investigatory and enforcement actions (Nesbitt 2003; Nevis Consulting Group 2003). As privacy custodians, ISPs must safeguard communications and personal information, and be accountable to their users regarding these practices. In their surveillance roles, ISPs collect and disclose information, and are sometimes prohibited from notifying their

users or the public of such activities. While those advocating for surveillance practices often claim that intermediaries can collect or disclose personal information while respecting privacy (Public Safety Canada 2012b, 371; Toews 2012), the contradiction between the two has been made clear through a number of legal contests covered in this article.

Surveillance by ISPs also occurs where it is profitable or aids in network management, and these practices must be reconciled with privacy commitments. Data generated about network users by ISPs has become increasingly lucrative, whether to target advertising, tailor services, authorize access, or to be transformed into new kinds of information commodities (Fung 2016). As ISPs expand their roles beyond merely carrying data, to collecting, and monetizing it as well, conflicts with privacy responsibilities can quickly arise (see Office of the Privacy Commissioner 2015b).

ISPs operate in the midst of rival pressures to collect and share more data on the one hand, and the concerns of users and privacy advocates on the other, where accommodating some desires or expectations creates tension with others. In steering a course through these currents, organizations must consider how their actions will be perceived, and so privacy governance is selectively publicized as a matter of corporate social responsibility (CSR, see Parsons 2017; Pollach 2011). Intermediaries seek to establish trust and confidence in their users, who understand that this relationship has the potential to be abused (Balkin 2016), and who are often concerned and distrustful about how their personal information is handled (Office of the Privacy Commissioner 2017). When intermediaries monetize personal information, they can try to win support from users by explaining the consumer benefits (Henderson 2014), or limit publicity and carry on "under the radar" (Behar 2018). Either way, obtaining valid consent from users is key in Canadian privacy law, and skirting this requirement can lead to the undesirable publicity of

public complaints and being called out by the Office of the Privacy Commissioner (2015b).

When ISPs share personal information without users' consent, as a result of pressure from state agencies or court orders, a common public justification is that these actions are limited to, or constrained by, what is legally required (Gaudrault 2012; Karadeglija 2014; Ling 2014; Mediacaster 2011). Whatever the public thinks of these practices, intermediaries insist they have no choice but to comply with the law. 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. Rogers* [2016]; *R. v. TELUS* [2013]). ISPs thereby minimize their agency, even as they exercise it. [3]

The final way for intermediaries to resolve their privacy role conflicts is to publicly position themselves as privacy champions, visibly going above and beyond a minimum commitment to PIPEDA. This is an approach that does not exclude the possibilities described above, as the same company can quietly monetize personal information, defend disclosures to government as a legal necessity, while also championing its efforts to fight for users' privacy interests. Positive actions by intermediaries are the focus of this article, but the roles of intermediaries as privacy custodians developed before PIPEDA and the internet, and this history requires some brief elaboration.

[3] 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, as justified by PIPEDA section 7(3)(c.1), are well-documented and admitted by the company elsewhere (TELUS 2014).

Pre-Internet Intermediaries as Privacy Custodians

While the expectations applied to intermediaries in Canada varied over the course of the nineteenth and twentieth century, 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 enforcement. By 1918, companies were subject to provincial legislation in Ontario and Quebec that regulated eavesdropping and wiretapping (Martin 1991, 144–145), followed in the 1950s by legislation in Alberta and Manitoba (Canadian Committee on Corrections 1969, 82; Cornfield 1967, 112). More general privacy laws developed gradually in Canada over the latter half of the twentieth century and into the twenty-first (Cohen 1982, 665–67; 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, 112). Rules prohibiting intermediaries divulging private communications could be overcome through some form of "lawful authority".[4] Intermediaries (specifically, telephone and telegraph companies) did apparently assist police investigations and enable wiretaps, but the extent and nature of this surveillance is unclear.[5]

In 1969 the *Ouimet Report* (Canadian Committee on Corrections 1969) recommended greater control over electronic surveillance and accountability for its use,

[4] Bell successfully opposed an Ontario Provincial Police warrant in 1947 and argued against a *Criminal Code* wiretap amendment in 1948. In the absence of legislation, police concluded that they themselves had the lawful authority to authorize a wiretap (Cornfield 1967, 113–114).

[5] From 1951 into the 1970s the RCMP maintained an extensive secret wiretapping program in cooperation with Bell and the British Columbia Telephone Company for national security purposes (Molinaro 2017). In 1969 the Chief of the Toronto Police stated that while his department had been tapping phones since 1966, they had "no formal, or informal, liaison with the telephone company on wiretapping, but added: 'The company does assist in other ways.'" (Burns 1969, p. 2). Sometimes wiretaps were installed without the phone company's knowledge, and the information obtained was generally not used as evidence in court (Burns 1969).

eventually leading to the *Protection of Privacy Act* in 1974 (Hubbard, Brauti, and Fenton 2015, sec. 1.1.1; Rabideau 1991, 172–73). The *Privacy Act* amended the *Criminal Code* to criminalize the "invasion of privacy" as well as formalizing the exemptions to such an offence. These exemptions specified when forms of electronic surveillance were not considered a crime, such as when carried out under judicial authorization (Hubbard, Brauti, and Fenton 2015). 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. By the 1990s, the legal authorities under which police could demand or request access to subscriber communications or records held by telephone companies were fairly clear, but the attempt to extend such rules to cover ISPs would set off lengthy and contentious debates.

Invisible Handshakes and Internet Surveillance

In the early public internet of the 1990s, police forces in general devoted little attention to online investigative and surveillance techniques. 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. In the 2000s, state agencies sought to make an "invisible

handshake" (Birnhack and Elkin-Koren 2003) 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 and Wu 2006, 73). Governments recognized that the cooperation of ISPs would be key to policing and surveillance in the online era, and some of these ISPs (the former telecom monopolies that emerged as ISPs in the mid-1990s) were already familiar partners for state agencies.

While some authors writing in the 2000s warned that ISPs would become close surveillance partners of state agencies (Birnhack and Elkin-Koren 2003) and copyright owners (de Beer and Clemmer 2009, 405–6), these authors did not fully appreciate the ways that the interests of these groups 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; Haggart 2014). 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 organizations 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.

Privacy and Piracy

In 2004 a group of incumbent ISPs took an active stand to protect the privacy of their

subscribers against a group of copyright owners. 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, ISPs had a statutory responsibility to limit the disclosure of personal information as a consequence of PIPEDA, which had recently come into effect. The Federal Court was in a position to decide between these competing demands, and had the power to order the ISPs to cooperate.

The relevant aspects of the case described above (known as *BMG Canada Inc. v Doe*), besides the threshold it established for subsequent information disclosures (Geist 2005), 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 and Cameron 2006, 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 information. The case would be an important early episode in a process which would see some intermediaries developing more positive conceptions 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 and Cameron 2006, 290; Pacienza 2004; Thompson 2004). This was a negative orientation to 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 (Pacienza 2004; Shaw 2004a, 2004b; Thompson 2004). 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, and TELUS (2004, 2) complained about being conscripted to carry out investigations for the copyright owners, which might result in the company being sued by its own customers (Kerr and Cameron 2006, 278–79).

In the end, Justice von Finckenstein refused to grant a court order to compel the ISPs to identify their customers on several grounds,[6] with Shaw and TELUS publicly claiming credit for protecting the privacy of their subscribers (Shaw 2004b). The decision (and its subsequent appeal) 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 (Geist 2005; Kerr and Cameron 2006).

While this particular episode is a good starting point for considering how ISPs

[6] The judge ruled that the evidence provided by MediaSentry was inadequate in linking file-sharing users and IP addresses. The Federal Court of Appeal upheld much of this reasoning, but changed to requirement for plaintiffs in future cases to present a "*bona fide"* rather than a "*prima facie"* claim to proceed with disclosure (Geist 2005).

developed into the privacy custodians upon which we are all now so dependent, 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 instance of ISPs asserting their positive responsibilities as privacy custodians in a way that established legal standards for future cases, 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). In a subsequent case involving the same copyright owner (Voltage Pictures), 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 2012), and argued for ways to minimize the privacy impacts of any information disclosure (TekSavvy 2015, 722–31). 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 (Distributel 2013, 52–54; O'Brien 2013). Most recently, in a case before the Supreme Court of Canada, Rogers has contested a motion from Voltage Pictures to identify its customers, but done so on the issue of costs rather than privacy grounds (Rose 2017).

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 statutory 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 responding to police agencies, PIPEDA's negative responsibilities have been more easily neutralized by exceptions written into the statute. Until the Supreme Court of Canada's decision in *R v. Spencer* [2014],[7] intermediaries had wide latitude to decide when to insist on a court order in law enforcement matters. Exceptions to privacy obligations, whether discretionary or mandatory, have been key points of contention in the story of lawful access in Canada.

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 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

[7] In *R v. Spencer* [2014] the Court unanimously decided that, except in very limited circumstances, disclosure of subscribers' personal information to police required a court order.

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 and O'Donoghue 2009, 34–35; Power 2013, 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), 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, 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, 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 in 2005 as a partnership between incumbent ISPs, industry associations, and government agencies (CCAICE 2005). 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, 8). The protocol provided a way for child exploitation investigators who had obtained an IP address to request an internet subscriber's name and address information at the "pre-warrant stage" of investigations (Morin 2011, 1). 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.

Since the phrase "lawful authority" was never clearly defined, it ended up being interpreted in different ways by government agencies and private organizations (House of Commons Standing Committee on Access to Information, Privacy and Ethics 2007; Lawson 2011; Morin 2011; L. Singer 2012). Disclosures were made in cases not involving child exploitation, and police sometimes requested more than just name and address information (Ling 2014; Office of the Privacy Commissioner 2015a, 7). While in some cases, a simple phone call from a police officer requesting information was enough for an intermediary to share its records, other organizations set the bar higher, and a small number refused any compromise of user privacy unless mandated by law. An intermediary's resistance could be grounded in a commitment to its users (Public Safety Canada 2012b, 271) or concerns over corporate liability for privacy violations (House of Commons Standing Committee on Access to Information, Privacy and Ethics 2007; Public Safety Canada 2012b, 184, 193). 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 2012b).

After successive governments failed to pass lawful access legislation, ISPs' discretion was curtailed by the Supreme Court's *Spencer* decision (*R. v. Spencer* [2014]), which strengthened privacy custodians' negative responsibilities and effectively barred most voluntary disclosures under PIPEDA's section 7(3)(c.1)(ii). However, the role conflict faced by intermediaries serving the needs of government agencies and acting as privacy custodians for their users remains an underlying tension.

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 2012b, 371; Toews 2012). 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. 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 2012b, 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 (Cavoukian 2011; Public Safety Canada 2012b, 2013a, 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, 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, with the choice to extend either privacy protection or government cooperation to the legal limit. The limits of what an intermediary could do in one of these roles would end up defining the other.

In general, intermediaries avoided taking a public position on either side of the lawful access debate. Industry representatives accepted government needs as legitimate, but made their support conditional on having specific concerns addressed (Public Safety Canada 2012b, 165, 257). Telecom companies were primarily interested in clearly determining their obligations under privacy law and lawful access legislation, and wanted to know how legal changes would impact their operations. The industry's main concerns were over the costs and obligations of lawful access (CBC News 2009; Nevis Consulting Group 2003; Parsons 2015, 263; Public Safety Canada 2011), and not over whether lawful access would make them less effective as privacy custodians. 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 (Braga 2016).

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, it is only since the latest lawful access consultation in 2016 that some intermediaries have championed privacy interests in public policy (Braga 2016; Solomon 2016). Before this, there are a number of ways in which some intermediaries have 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 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 2016), and differentiating themselves from other companies that have presumably complied with similar orders (see Fraser 2016).

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 2016). 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 has been supported by many Canadian ISPs.

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 and security. 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 more openly communicating corporate privacy practices.

One significant development toward a more positive role for intermediaries as privacy custodians has come in the form of "transparency reports", and greater disclosure of these companies' role in facilitating state surveillance. Since 2010, numerous (primarily US-based) companies have been issuing such transparency reports, documenting how they handle requests from both governments and private actors to remove content or disclose information (Clement and Obar 2016, 300). Canadian intermediaries 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 (Bronskill 2014; Freeze, Dobby, & Wingrove 2014). Even so, the release of the first of such reports in 2014 came in the absence of an immediately precipitating crisis, scandal, or "sudden focusing event" in Canada's telecom industry (Parsons 2017, 11). TekSavvy and Rogers were the first to publish reports, despite the role conflict created through contradictory lawful access responsibilities that appeared to restrict such disclosures, with Rogers effectively declaring a new approach to privacy and surveillance in which "the needs of [Rogers] customers came first" (Bronskill

2014).[8]

Industry Canada responded to this private sector initiative by producing guidelines for transparency reports (Industry Canada 2015), thereby contributing to their legitimization, and the majority of Canada's large telecom companies (with the notable exception of Bell) now account for disclosures of personal information in some form. However, standardization of reporting across the industry has not taken place and companies can be selective in how they report on privacy governance. Rather than leveling the information asymmetry between users and ISPs and enabling comparisons across the industry, transparency reports can be used to enhance an organization's reputation or public image (Parsons 2017). This is significant in and of itself however, as it demonstrates how privacy accountability is reputation-enhancing enough to pursue – in this case normalizing a practice that goes beyond statutory obligations.

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

[8] In 2014 some intermediaries expressed concerns that regulations prevented them from disclosing information about lawful access. While TELUS sought government clarification (Bronskill 2014), TekSavvy and Rogers published their reports without consulting government. Rogers` Ken Engelhart remarked in an interview that "there was too much sensitivity in the past about not wanting to upset law enforcement officials" (Freeze, Dobby, & Wingrove, 2014).

"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" (2016).

These higher expectations for privacy custodians can be contradicted by legislation to grant police greater powers or to limit liability for disclosure (see Handa, Birbilas & Fazio, 2015), but a more immediate contradiction has arisen from intermediaries' business opportunities to collect and exploit personal information (Fung 2016). Bell stepped into a new advertising role and expanded its collection of personal information in 2013 to include its subscribers' internet browsing habits (Henderson 2014). Following an unprecedented number of complaints, the Office of the Privacy Commissioner (2015b) found that Bell had not obtained adequate consent from its customers, leading the company to withdraw the program and delete the collected information (Dobby 2015). More recently, a privacy scandal in the U.S. led to publicity for EnStream, which is jointly owned by Bell, Rogers and TELUS to serve clients interested in verifying subscriber identities or determining the locations of users (Behar 2018). In these cases, intermediaries play a double role by providing subscribers with connectivity and privacy, while providing another set of customers a service that depends on user data. These roles can largely be reconciled with statutory obligations by satisfying the requirement for expressed consent from subscribers, but an intermediary that profits from what it knows about individuals has a qualitatively different relationship with subscribers than an intermediary that limits any non-essential collection and disclosure.

The future outlook for intermediaries as privacy custodians is therefore quite mixed. The *Spencer* decision has restricted voluntary disclosures of personal information to government agencies, and with the exception of obligations for companies experiencing a data breach

(Lithwick 2014), new positive responsibilities have not been imposed through law. Nevertheless, a number of intermediaries have 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, with organizations choosing to exceed minimum privacy obligations only in particular ways. Therefore, we should expect to see privacy custodians to continue differentiating themselves on the basis of their positive conduct, but doing so in a selective manner. Future scandals may add to the current public unease around privacy governance by corporations (Angus Reid Institute 2018; Office of the Privacy Commissioner 2017) and generate more comprehensive approaches by privacy custodians to meet consumer expectations.[9] In the immediate future we should be alert to how intermediaries respond to continuing pressures to monetize private information. Finally, the old tensions around lawful access remain, and battle lines around the issue may be drawn again if advocates are able to successfully move it back onto the government's policy agenda (Parsons 2015).

Conclusion

Intermediaries now occupy a pivotal role as privacy custodians, but this is by no means a culmination of the hundred-year history outlined earlier in this paper. Public policies to safeguard privacy took time to develop, and did so in close relation to contradictory pressures. Relevant legal regimes have sometimes imposed clear obligations and prohibitions, but

[9] Privacy custodians could further distinguish themselves through policy advocacy, commitments about data routing, storage, and retention, as well as more detailed information about their procedures for disclosing personal information (Clement and Obar 2016).

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 organizations 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. Through their interaction with government agencies – in government consultations, through collaborative alliances like the CCAICE, and in court or regulatory battles – ISPs have played an important part in determining what privacy governance means for individual users.

I have argued that the responsibilities of privacy custodians can be differentiated in positive and negative terms. Negative responsibilities, or prohibitions on particular kinds of conduct, typically include exceptions that have been at the center of role conflicts, public debates, and court cases involving ISPs. These exceptions include PIPEDA's section 7(3)(c.1), which allowed for otherwise-prohibited disclosures of personal information. Court orders in copyright cases are an exception that mandates such disclosures. Consent can also free a company from certain responsibilities if it is properly obtained.

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, and being more open about how they govern privacy, such as through transparency reports. Intermediaries raising the bar through positive responsibilities have been a welcome development, and an important counterbalance to forces

pushing in the opposite direction.

There is no neat distinction between privacy custodians that take a positive orientation and those that meet the bare minimum of their obligations. Privacy responsibilities are diverse and each ISP can choose which statutory obligations to exceed. The same organizations that champion privacy through one set of actions might collect, use and disclose personal information through others, selectively publicizing only those efforts that enhance their reputations as privacy custodians. These different choices can be distinguished and compared to better inform consumers, but any such evaluation is limited by what ISPs decide to disclose about their practices, and customers' ability to choose in a concentrated market (Clement and Obar 2016).

We know from previous experience that role conflicts occur where the responsibilities of a privacy custodian and state surveillance partner must be 'balanced', and additional conflicts will likely arise as ISPs find new uses for information about their users. While there are now compelling reasons for intermediaries to present themselves as being responsible, trustworthy and even trailblazing when it comes to governing privacy, we are still largely dependent on what these organizations tell us about their actions and policies. The recent trend towards greater transparency has provided more information about how we are governed by these indispensable institutions, but also highlighted their continued discretion in disclosing information about themselves. An organization that acts positively in some respects will not do so in all others, and practices that users might disapprove of are less likely to be publicized.

In an era of growing concern over personal privacy (Office of the Privacy Commissioner 2017), amidst stories of data breaches, surveillance and behavioral manipulation, the conduct of privacy custodians is of major public importance. Intermediaries can be expected to express their own positions in the policy debates of the future, but it is less clear whether they will attempt to

speak on behalf of users' privacy interests. As the lawful access battle over Bill C-30 demonstrated, it may be necessary for public voices to articulate their own demands. Researchers and regulators have their own role to play in cutting through information asymmetries and advancing these debates, which will continue to delimit and influence privacy custodians' decisions.

Cases Cited

BMG Canada Inc. v. John Doe [2004], 3 FCR 241.

R. v Rogers Communications [2016]. ONSC 70.

R. v. Spencer [2014]. SCC 43.

R. v. TELUS [2013]. 2 SCR 3.

R v. Weir [1998]. ABQB 56.

Statutes

Canadian Security Intelligence Service Act, RSC 1985, c C-23.

Competition Act, RSC 1985, c C-34.

Criminal Code, RSC 1985, c C-46.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Protection of Privacy Act, SC 1973-4, c 50.

References

Abdelnour, Samer, Hans Hasselbladh, and Jannis Kallinikos. 2017. "Agency and Institutions in Organization Studies." *Organization Studies* 38 (12): 1775–92.

Angus Reid Institute. 2018. "Un-Liking Facebook: 3-in-4 Canadian Users Say Data Mining Scandal Will Change How They Use the Platform." *Angus Reid Institute*. March 26. http://angusreid.org/facebook-cambridge-analytica-tech/.

Balkin, Jack M. 2016. "Information fiduciaries and the first amendment." *U.C. Davis Law Review* 49 (4): 1183-1234.

BCCLA. 2012. "Moving Towards a Surveillance Society: Proposals to Expand 'Lawful Access'

in Canada." *BC Civil Liberties Association*. January 13. http://www.bccla.org/wp-content/uploads/2012/03/2012-BCCLA-REPORT-Moving-toward-a-surveillance-society.pdf.
Behar, Rose. 2018. "Here's How Bell, Rogers and Telus Profit from Your Mobile Subscriber Data." *MobileSyrup*. May 18. https://mobilesyrup.com/2018/05/18/bell-telus-rogers-sell-location-data-third-parties-enstream/.
Bell. 2004. "Written Representations." March 11. https://cippic.ca/sites/default/files/file-sharing-lawsuits/Bell_Written_Submissions.pdf.
Birnhack, Michael D., and Niva Elkin-Koren. 2003. "The Invisible Handshake: The Reemergence of the State in the Digital Environment." *Virginia Journal of Law and Technology* 8 (2): 1–57.
Blackburn, Shelly. 2013. "Proud of Our Commitment to Privacy in Canada." *TELUS Blog*. August 7. http://blog.telus.com/public-policy/proud-of-our-commitment-to-privacy-in-canada/.
Braga, Matthew. 2016. "Canadian Telecoms Push Back on Proposed Police Powers." *CBC News*. December 20. http://www.cbc.ca/news/technology/rogers-teksavvy-itac-cwta-bill-c51-national-security-1.3903930.
Bronskill, Jim. 2014. "Feds Were Worried as Telecom Firm Planned to Go Public on Police Access to Canadians' Phone Calls and Emails, Memo Shows." *National Post*. December 1. 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.
Burns, John. "58 Wiretaps Last Year, Mackey Says." *Globe and Mail*, June 27, 1969.
Canadian Committee on Corrections. 1969. *Recommendations of the Canadian Committee on Corrections [Ouimet Report]*. Ottawa: The Queen's Printer. http://www.johnhoward.ca/media/%281969%29%20HV%208395%20A6%20C33%201969%20%28Ouimet%29.pdf.
Canadian Press. 2012. "Online Snooping Bill Creates 'Inspectors' With Unfettered Access To Internet Records: Report." *The Huffington Post*. February 17. http://www.huffingtonpost.ca/2012/02/17/lawful-access-telecoms_n_1284120.html.
Cavoukian, Ann. 2011. "Lawful Access." *The Globe and Mail*, December 6, sec. Letter to the Editor.
CBC News. 2009. "ISPs Must Help Police Snoop on Internet under New Bill." June 18. http://www.cbc.ca/news/technology/isps-must-help-police-snoop-on-internet-under-new-bill-1.817756.
CCAICE. 2005. "Canadian Coalition Against Internet Child Exploitation Releases National Action Plan," May 11. https://www.cybertip.ca/app/en/media_release_ccaice_action_plan.
Clement, Andrew, and Jonathan A. Obar. 2016. "Keeping Internet Users in the Know or in the Dark: An Analysis of the Data Privacy Transparency of Canadian Internet Carriers." *Journal of Information Policy* 6: 294–331.
Cohen, Stanley A. 1982. "Invasion of Privacy: Police and Electronic Surveillance in Canada." *McGill Law Journal* 27 (November): 619–75.
Cornfield, David A. 1967. "The Right to Privacy in Canada." *Faculty of Law Review (University of Toronto)* 25: 103–20.
CRTC. 2009. "Telecom Regulatory Policy 2009-723." *Canadian Radio-television and*

Telecommunications Commission. November 25. http://www.crtc.gc.ca/eng/archive/2009/2009-723.htm.
de Beer, Jeremy F., and Christopher D. Clemmer. 2009. "Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?" *Jurimetrics* 49 (4): 375–409.
Distributel. 2013. "Motion Record of Distributel Communications Limited." http://www.scribd.com/doc/124826637/Motion-Record-of-Distributel-Communications-Limited.
Dobby, Christine. 2012. "TekSavvy Illegal Downloading: Judge Awards More Time to Warn Clients." *Financial Post*. December 17. http://business.financialpost.com/2012/12/17/judge-gives-teksavvy-more-time-to-warn-customers-of-illegal-downloading-copyright-case/.
———. 2015. "Bell Canada to Revamp Online Ad Program to Allow Upfront Consent." *The Globe and Mail*. April 13. http://www.theglobeandmail.com/report-on-business/bell-canada-to-revamp-online-ad-program-to-allow-upfront-consent/article23901505/.
———. 2016. "Ontario Court Rules Police Orders Breached Cellphone Users' Charter Rights." *Globe and Mail*. January 14. http://www.theglobeandmail.com/report-on-business/industry-news/the-law-page/court-sides-with-telecoms-in-landmark-cellphone-privacy-case/article28180968/.
Edwards, Lilian. 2011. "Role and Responsibility of the Internet Intermediaries in the Field of Copyright and Related Rights." Report. Geneva: WIPO. http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf.
Fraser, David. 2016. "Tower Dump Case Raises Troubling Questions about Law Enforcement and Privacy." *Canadian Privacy Law Blog*. January 18. http://blog.privacylawyer.ca/2016/01/tower-dump-case-raises-troubling.html.
Freeze, Colin, Christine Dobby, and Josh Wingrove. "TekSavvy, Rogers Break Silence over Government Requests for Data." *The Globe and Mail*, June 5. http://www.theglobeandmail.com/technology/tech-news/teksavvy-opens-books-on-government-data-requests/article18999107/.
Fung, Brian. 2016. "Internet Providers Want to Know More about You than Google Does, Privacy Groups Say." *The Washington Post*, January 20. 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/.
Gaudrault, Marc. 2012. "Why We Are Not Opposing Motion on Monday." *DSLReports Forums: TekSavvy*. http://www.dslreports.com/forum/r27824891-Why-we-are-not-opposing-motion-on-Monday.
Geist, Michael, ed. 2005. *Internet and E-Commerce Law in Canada* 6 (5). https://web.archive.org/web/20180320230726/http://www.macerajarzyna.com/pages/publications/BMG%20Case%20-%20E-Commerce.pdf.
———. 2016. "Why Your Telecom Must Defend Your Right to Privacy." *The Toronto Star*, January 25. http://www.thestar.com/business/2016/01/25/why-your-telecom-must-defend-your-right-to-privacy-geist.html.
Goldsmith, Jack L., and Tim Wu. 2006. *Who Controls the Internet?: Illusions of a Borderless World*. Oxford: Oxford University Press.
Government of Canada. 2002. "Lawful Access – Consultation Document." August 25.

http://www.justice.gc.ca/eng/cons/la-al/consult.html.
Haggart, Blayne. 2014. *Copyfight: The Global Politics of Digital Copyright Reform*. Toronto: University of Toronto Press.
Handa, Sunny, Laurie Birbilas, and Justina Di Fazio. 2015. "Bill C-13: Cyberbullying Bill Introduces New Lawful Access Measures." *Blakes Bulletin*. January 23. http://www.blakes.com/English/Resources/Bulletins/Pages/Details.aspx?BulletinID=2057.
Henderson, Peter. 2014. "Bell Defends Targeted Ad Program as 'Transparent.'" *The Wire Report*. April 30. http://www.thewirereport.ca/news/2014/04/30/bell-defends-targeted-ad-program-as-%E2%80%98transparent%E2%80%99/28217.
House of Commons Standing Committee on Access to Information, Privacy and Ethics. 2007. "Transcript of Meeting No. 30, February 13, 2007." February 13. http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=2695445&Language=E&Mode=1.
Hubbard, Robert W., Peter M. Brauti, and Scott K. Fenton. 2015. *Wiretapping and Other Electronic Surveillance: Law and Procedure*. Toronto: Thomson Reuters.
Ibbitson, John. 2012. "How the Toews-Sponsored Internet Surveillance Bill Quietly Died." *The Globe and Mail*. May 15. http://www.theglobeandmail.com/news/politics/how-the-toews-sponsored-internet-surveillance-bill-quietly-died/article4179310/.
Industry Canada. 2015. "Transparency Reporting Guidelines." June 30. http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html
Karadeglija, Anja. 2014. "Telecoms Don't Give out Customer Info 'Willy-Nilly': Bell Ombudsman." *The Wire Report*. May 2. 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.
Kerr, Ian. 2002. "In the Year 2000: Me and My ISP." In *Personal Relationships of Dependence and Interdependence in Law*, edited by Law Commission of Canada, 78–119. Vancouver, BC: UBC Press.
Kerr, Ian, and Alex Cameron. 2006. "NYMITY, P2P & ISPS: Lessons from BMG Canada Inc. v. John Doe." In *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, edited by Katherine J. Strandburg and Daniela Stan Raicu, 269-. New York: Springer.
Lawson, Philippa. 2011. "Bill C-12 and 'Lawful Authority' under PIPEDA." *Slaw*. November 23. http://www.slaw.ca/2011/11/23/bill-c-12-and-lawful-authority/.
Lawson, Philippa, and Mary O'Donoghue. 2009. "Approaches to Consent in Canadian Data Protection Law." In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr, Carole Lucock, and Valerie Steeves, 399–416. Oxford: Oxford University Press. http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_22.pdf.
Ling, Justin. 2014. "For Canada's Spies, Your Data Is Just a Phone Call Away." *Vice - Motherboard*. May 15. http://motherboard.vice.com/read/canadian-spies-can-look-at-your-user-data-consequence-free.
Lithwick, Dara. 2014. "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." *Library of Parliament*. June 11. http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/41/2/s4-e.pdf.
Martin, Michèle. 1991. *Hello, Central?: Gender, Technology, and Culture in the Formation of*

Telephone Systems. Montreal: McGill-Queen's Press.
McKenna, Alain. 2011. "Téléchargement de The Hurt Locker: Des Internautes Canadiens Poursuivis." *La Presse*. November 28. http://techno.lapresse.ca/nouvelles/internet/201111/28/01-4472247-telechargement-de-the-hurt-locker-des-internautes-canadiens-poursuivis.php.
Mediacaster. 2011. "Canadian ISPs to Deliver Customer Information in Hurt Locker Lawsuit." *Mediacaster Magazine*. September 9. 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. "MediaSmarts." http://mediasmarts.ca/.
Miller, Claire Cain. 2014. "Revelations of N.S.A. Spying Cost U.S. Tech Companies." *The New York Times*, March 21. http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.
Molinaro, Dennis. 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* 93 (3): 457–82.
Morin, Suzanne. 2011. "Updated: Business Disclosure of Personal Information to Law Enforcement Agencies: PIPEDA and the CNA Letter of Request Protocol." *Privacy Pages*, November. http://www.cba.org/cba/newsletters-sections/pdf/2011-11-privacy1.pdf.
Neocleous, Mark. 2008. *Critique of Security*. Edinburgh: Edinburgh University Press.
Nesbitt, Scott. 2003. "Rescuing the Balance? An Assessment of Canada's Proposal to Limit ISP Liability for Online Copyright Infringement." *Canadian Journal of Law and Technology* 2: 115–28.
Nevis Consulting Group. 2003. "Summary of Submissions to the Lawful Access Consultation." August 6. http://canada.justice.gc.ca/eng/cons/la-al/sum-res/index.html.
O'Brien, Greg. 2013. "Independent ISP Distributel Fighting Moviemakers over Customer Privacy." February 14. 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." http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
Office of the Privacy Commissioner. 2014. "Metadata and Privacy - A Technical and Legal Overview." October 30. https://www.priv.gc.ca/information/research-recherche/2014/md_201410_e.asp#ftnref27.
———. 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." A-2014-00158. http://paroxysms.ca/csis_random/csis_cyberwar.pdf.
———. 2015b. "Results of Commissioner Initiated Investigation into Bell's Relevant Ads Program." April 7. https://www.priv.gc.ca/cf-dc/2015/2015_001_0407_e.asp.
———. 2015c. "Transparency Reporting by Private Sector Companies: Comparative Analysis." June 30. https://www.priv.gc.ca/information/research-

recherche/2015/transp_201506_e.asp.
———. 2017. “2016 Survey of Canadians on Privacy.” January 26, 2017. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/#fig16.
Pacienza, Angela. 2004. “Cdn Recording Industry Begins Legal Fight to Stop Music Uploaders.” *Canadian Press*, February 16.
Parsons, Christopher. 2015. “Stuck on the Agenda: Drawing Lessons from the Stagnation of ‘Lawful Access’ Legislation in Canada.” In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, edited by Michael Geist, 257–83. Ottawa: University of Ottawa Press. http://www.ruor.uottawa.ca/bitstream/10393/32424/1/9780776621838_WEB.pdf.
———. 2017. “The (In)Effectiveness of Voluntarily Produced Transparency Reports.” *Business & Society*.
Pollach, Irene. 2011. “Online Privacy as a Corporate Social Responsibility: An Empirical Study.” *Business Ethics: A European Review* 20 (1): 88–102.
Power, E. Michael. 2013. *The Law of Privacy*. Markham: LexisNexis.
Public Safety Canada. 2011. “Summary of Public Consultation on Access to Customer Name and Address Information for Public Safety Purposes.” October 22. http://www.publicsafety.gc.ca/prg/ns/sum-conslt-eng.aspx.
———. 2012a. “All Records from March 1 to November 4, 2011 about Canada’s Privacy Commissioners’ Positions on the Proposed Lawful Access Bills.” A-2011-00220.
———. 2012b. “Records on Government Consultations with Law Enforcement and Justice Officials Concerning the Negative Impact of a Warrant Requirement for Basic Subscriber Information.” A-2011-00255. https://telecomtransparency.org/wp-content/uploads/2015/07/A-2011-00255.pdf.
———. 2013a. “Correspondence from the Public on Bill C-30 from Feb 1 May 10, 2012.” A-2012-00301.
———. 2013b. “Records Concerning Bill C-30 Currently before Parliament, from Oct 1 to Dec 3, 2012.” A-2012-00333.
Rabideau, Monique. 1991. “Duarte v. R.: In Fear of Big Brother.” *University of Toronto Faculty of Law Review* 49: 171–85.
Rogers. 2004. “Written Representations of Rogers Communications Inc.” March 12. https://cippic.ca/sites/default/files/file-sharing-lawsuits/Rogers_Written_Reps_Mar12.pdf.
Rose, Keith. 2017. “SCC To Weigh In On Fees For Identifying ISP Subscribers: Rogers v. Voltage,” *SnIP/ITs*, November 24. https://www.canadiantechlawblog.com/2017/11/24/scc-to-weigh-in-on-fees-for-identifying-isp-subscribers-rogers-v-voltage/.
Shaw. 2004a. “Written Representations of Shaw Communications Inc.” March 10. https://cippic.ca/sites/default/files/file-sharing-lawsuits/FurtherWrittenSubmissionsShaw.pdf.
Shaw, Gillian. 2004b. “Sharing Music over Internet Not Illegal, Federal Court Rules.” *The Vancouver Sun*, April 1, sec. News.
Singer, Leo. 2012. “Unwarranted Access?” *National*, July. http://www.nationalmagazine.ca/Articles/June-2012-Issue/Unwarranted-access.aspx.
Singer, Marcus G. 1965. “Negative and Positive Duties.” *The Philosophical Quarterly* 15 (59): 97–103.

Solomon, Howard. 2016. “Protect Privacy of Subscribers, but Don’t Stick Us with the Bill, CWTA Tells Ottawa.” *Cartt.Ca*. December 6. https://cartt.ca/article/protect-privacy-subscribers-don%E2%80%99t-stick-us-bill-cwta-tells-ottawa.

Stoddart, Jennifer, Frank Work, Elizabeth Denham, Irene Hamilton, Anne E. Bertrand, Ed Ring, Elaine Keenan Bengts, et al. 2011. “Letter to Public Safety Canada from Canada’s Privacy Commissioners and Ombudspersons on the Current ‘Lawful Access’ Proposals.” March 9. https://www.priv.gc.ca/media/nr-c/2011/let_110309_e.asp.

Stryker, Sheldon. 1980. *Symbolic Interactionism: A Social Structural Version*. Menlo Park: Benjamin-Cummings.

TekSavvy. 2015. “Transcript Brief.” November 5. https://cippic.ca/sites/default/files/CF_No._T-2058-12_-_TekSavvy_ats_Voltage_-_Transcript_Brief.pdf.

TELUS. 2004. “Written Representations.” March 11. https://cippic.ca/sites/default/files/file-sharing-lawsuits/Written_Representations.pdf.

———. 2014. “TELUS Transparency Report 2013.” http://about.telus.com/servlet/JiveServlet/downloadBody/5544-102-1-6081/TELUS%20Transparency%20Report%202013%20-English.pdf

———. 2016. “Telus WISE.” *Telus WISE*. http://wise.telus.com/.

Thies, Cameron G., and Marijke Breuning. 2012. “Integrating Foreign Policy Analysis and International Relations through Role Theory.” *Foreign Policy Analysis* 8 (1): 1–4.

Thompson, Robert. 2004. “Shaw Won’t Breach Privacy to Nab Net Pirates: Music Industry Taking Case to Court.” *Edmonton Journal*, February 14, sec. News.

Toews, Vic. 2012. “House of Commons Debates.” *Openparliament.Ca*. February 28. https://openparliament.ca/debates/2012/2/28/vic-toews-1/.

Valiquet, Dominique. 2011. “Legislative Summary of Bill C-22: An Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons Who Provide an Internet Service.” February 15. http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?Language=E&ls=c22&Parl=40&Ses=3&source=library_prb.

Woods, Allan. 2014. “Canada Courting U.S. Web Giants in Wake of NSA Spy Scandal.” *The Toronto Star*, January 9. http://www.thestar.com/news/canada/2014/01/09/us_companies_look_to_canadian_servers_in_wake_of_nsa_spy_scandal.html.