David Asper Centre for Constitutional Rights
UNIVERSITY OF TORONTO

Submissions to the Office of the Privacy Commissioner of Canada Regarding Lawful Access and the Consent Model under *PIPEDA*

Contributors:

Dr. Lisa M. Austin
Associate Professor, University of Toronto Faculty of Law

Executive Director Cheryl Milne and Research Assistant Geneviève Ryan
David Asper Centre for Constitutional Rights

Date: July 28, 2016

About the David Asper Centre for Constitutional Rights

The David Asper Centre for Constitutional Rights is a centre within the University of Toronto, Faculty of Law devoted to advocacy, research and education in the area of constitutional rights in Canada. The Centre houses a unique legal clinic that brings together students, faculty and members of the legal profession to work on significant constitutional cases. Through the establishment of Centre the University of Toronto joins a small group of international law schools that play an active role in constitutional debates of the day. It is the only Canadian Centre in existence that attempts to bring constitutional law research, policy, advocacy and teaching together under one roof. The Centre aims to play vital role in articulating Canada's constitutional vision to the broader world. The Centre was established through a generous gift to the law school from U of T law alumnus David Asper (LLM '07).

About Dr. Lisa Austin

Dr. Lisa Austin, Ba & Sc (McMaster) 1994, MA (Toronto) 1995, LLM Toronto (1998), PhD (Toronto) 2005, called to the Bar of Ontario in 2006, is an Associate Professor. Prior to joining the faculty, she served as law clerk to Mr. Justice Frank Iacobucci of the Supreme Court of Canada. Her privacy work has been cited numerous times by Canadian courts, including the Supreme Court of Canada. Most recently, she collaborated on a report for the Office of the Privacy Commissioner of Canada entitled *Seeing Through the Cloud: National Jurisdiction and Location of Data, Servers and Networks Still Matter in a Digitally Interconnected World.* Previous policy work includes consulting for the Canadian Judicial Council on their *Model Policy for Access to Court Records in Canada.*

Summary of Recommendations

These submissions were prepared by Dr. Lisa Austin and the David Asper Centre for Constitutional Rights in response to the call for submissions from the Office of the Privacy Commissioner of Canada on the consent model under the *Personal Information and Protection of Electronic Documents Act (PIPEDA)*. The consultation questions that are the focus of these submissions are: what roles, responsibilities and authorities should the parties responsible for promoting the development and adoption of solutions have to produce the most effective system, and what, if any, legislative changes are required? We make two main recommendations:

1) The disclosure of personal information for law enforcement, investigative or national security purposes should be subject to review that reflects the protection of s.8 *Charter* rights and not simply be reviewed on a reasonableness or necessity standard.
2) The Office of the Privacy Commissioner should take a more proactive role in *PIPEDA* oversight.

These recommendations do not require any legislative change. Rather, they require an approach to existing legislation that recognizes the interconnectedness of *PIPEDA* with individual *Charter* rights, and a more proactive use of the Office of the Privacy Commissioner's existing abilities and responsibilities.

Introduction: The Public/Private Nexus of State Surveillance

As Bruce Schneier argues in his recent book, *Data and Goliath*, we are living in an age where "corporate and government surveillance interests have converged."[1] Any discussion of the reform of Canada's *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[2] must take this into account. We can no longer isolate privacy protection into various "silos" where we think about how to regulate the private sector in isolation from considerations about state access to the information the private sector collects. The question of lawful access to personal information, and its *Charter* dimensions, is a crucial element of the degree to which the regulation of private sector information practices protects privacy rather than enable surveillance. This must be part of any discussion of *PIPEDA*'s consent requirements.

Our submission focuses on two aspects of *PIPEDA*: exceptions to consent requirements for lawful access requests under s. 7(3), and the reasonable purposes requirement for the collection, use and disclosure of personal information under s. 5(3).

Our submission begins with an overview of the statutory framework for lawful access requests under s. 7(3) and recent applications of that framework by the court. This overview will demonstrate that exceptions to the consent requirements under *PIPEDA* are broadly worded and give ambiguous guidance in assessing the constitutional validity of lawful access requests or other disclosures. Our overview of recent jurisprudence on law enforcement requests for disclosure of personal information and cell tower record production orders illustrates the difficulties in applying *PIPEDA's* ambiguous requirements to state action. Lawful access requests should operate by clear legal requirements, either through constitutionally valid warrants or clear statutory exceptions to the warrant requirement. Disclosure of personal information under *PIPEDA* must be subject to a review reflective of the protection of s.8 *Charter* rights, not simply a review on a reasonableness or necessity standard. We also argue that the Office of the Privacy Commissioner must take on a more proactive role in reviewing the privacy policies and information practices of private organizations.

Part I Lawful access under *PIPEDA*

1) Lawful Access

The primary means by which *PIPEDA* protects personal information is through knowledge and consent. S. 5(1) of *PIPEDA* provides that "every organization shall comply with the obligations set out in Schedule 1",[3] including knowledge and consent, subject to certain exceptions.

Under s.6.1 of *PIPEDA*, consent is deemed valid only where "it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting."[4]

---

[1] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (2015) at 25.
[2] SC 2000, c 5 [*PIPEDA*].
[3] *Ibid,*, s.5(1).
[4] *Ibid.,* s.6.1.

Exceptions to the consent requirement for the collection, use and disclosure of personal information are provided under s. 7 of *PIPEDA*. As our submission focuses on lawful access to personal information, we will only address the exceptions to consent for disclosure of personal information under s. 7(3) of the Act. Lawful access by state authorities is provided for under ss. 7(3)(c) and 7(3)(c.1)(i-iii) of *PIPEDA*. Under these provisions, an individual's private information may be disclosed by a private organization without the consent of the individual when:

> s.7(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is
>
> ...
>
> (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information…
>
> (c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
>
> (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
>
> (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,
>
> (iii) the disclosure is requested for the purpose of administering any law of Canada or a province

While s. 7(3)(c) clearly requires a warrant or similar court order, the extensive exceptions under s. 7 (3)(c.1)(i-iii) are ambiguous. The purposes of national security, international affairs and law enforcement are all very broad. It is not clear from the wording in *PIPEDA* what it means for a state actor to 'identify its lawful authority' or what constitutes 'lawful authority' to access the requested information. The word 'requested' implies that the disclosure may be made voluntarily by the organization – that is, without being given a warrant or order for the production of the information.

What is clear from the wording of s. 7(3) is that the lawful access provisions are meant to be limited exceptions to the general rule of knowledge and consent. The accompanying note mentioned in s. 7(3) identifies circumstances in which personal information may be collected, used or disclosed without consent. The wording "despite the note that accompanies that clause" demonstrates the importance that legislators placed on ensuring that exceptions to knowledge and consent requirements are limited. The Federal Court has also interpreted s.7(1) as exhaustively setting out exceptions to the obligation to ensure knowledge and consent.[5]

[5] *Wansink v Telus Communications Inc*, 2007 FCA 21 at para 23.

Private organizations today collect extensive information on the individuals accessing their products or services. As made clear by the jurisprudence discussed below, this information can include name and contact information, billing information, details of Internet usage and cell phone communications and geographical information revealing their location at the time the service was used. Communications, usage and geographical information are commonly known as 'metadata': information generated by the use of technology, the analysis of which can lead to the identification of the "who, what, where, when and how of a variety of activities."[6] While metadata has traditionally been thought to be less informative than strict 'content' data (for example, the actual contents of a message or phone call), technological and analytical advances are blurring this distinction and leading to a growing consensus about the important privacy implications of metadata.[7] That this information could be useful in the context of law enforcement or national security operations is obvious. That the same information has the potential to be highly personal and revelatory of an individual's private activities is becoming increasingly obvious.

Lawful access to personal information held by third parties should not operate through voluntary compliance with state requests. Instead, such lawful access should only occur where the law clearly *requires* it. This could be through constitutionally valid warrants or production orders, or it could be through statutory provisions that are constitutionally valid exceptions to the standard warrant requirement. In this way, lawful access is subject to judicial scrutiny and review as well as democratic accountability rather than being subject to the discretion of private sector organizations with limited public transparency. This requirement will give effect to the primary purpose of *PIPEDA* – to protect an individual's personal information and ensure that disclosure without consent remains a limited exception to the general rule.

2) The reasonableness requirement

Under *PIPEDA* private organizations also have the responsibility of limiting the collection, use and disclosure of information from individuals to what is "reasonable". This obligation is found in s. 5(3) of *PIPEDA*:

> s. 5(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

This standard is essentially one of justification. In a scenario where a law enforcement or state authority requested disclosure of personal information from a private organization, s. 5(3) only asks whether the information is being requested for an 'appropriate purpose'. This is a much lower standard than the protection provided by s.8 of the *Charter*, which engages in a balancing of the state objective against the individual right to privacy. What the application of a reasonableness requirement does is bypass the constitutional questions raised by s.8 of the *Charter* and rushes to something more akin to a s.1 justification test.

---

[6] OPC, "What is Metadata?" (2014): https://www.priv.gc.ca/information/research-recherche/2014/md_201410_e.pdf, page 1.
[7] For a discussion of this, see Edward W. Felten's written testimony to the United States Senate, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act (October 2, 2013): http://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf. See also Information and Privacy Commissioner of Ontario, "A Primer on Metadata: Separating Fact from Fiction" (2013): https://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1316.

The balancing that takes place within s.8 is much stricter than an *Oakes*-like test with its emphasis on "minimal impairment". For example, the reasonable and probable grounds test under s.8 is one that contemplates that sometimes the state does *not* get access to the information it seeks even if this information is necessary for a law enforcement purpose. Under s.8, "[t]he idea is *not* that privacy must give way so long as it is intruded upon as minimally as possible but that law enforcement goals hold sway only at a particular point marked by the probable effectiveness of reaching that goal."[8] There are circumstances, therefore, where the disclosure of information that is considered 'reasonable' under *PIPEDA* will nonetheless violate the *Charter*.

This provision is especially important with respect to private organizations that employ service agreements or terms of use to govern their relationship with their clients. Internet service providers, cell phone carriers and software developers are all private organizations whose service agreements and acceptable use policies can be described as 'contracts of adhesion'. That is, they are non-negotiable contractual terms unilaterally imposed by the private organization on the individual as a precondition of the individual accessing the product or service being offered.

Privacy policies and user agreements of private organizations are at best ambiguous with regards to company policies surrounding state requests to information. Most simply state that they will only disclose a customer's personal information to third parties either with the consent of that customer or where that disclosure is "required by law" subject to *PIPEDA*.[9] These clauses rarely indicate a company practice of requiring a warrant before agreeing to a request for information disclosure.

These clauses have a direct impact on the constitutional rights of the individual vis-à-vis the state. For example, in *R v Godbout*[10] the BC Court of Appeal found that the recipient of a package had no reasonable expectation of privacy in the contents of that package because the shipping contract included a provision that the carrier or any government authority could search the package without notice. The shipping contract had been signed by the sender, not the recipient. Such language effectively reduces an individual's freedom from unreasonable search and seizure by affecting an individual's reasonable expectation of privacy under the *Charter*, at least according to some court interpretations. It should not be found reasonable, under s 5.(3) of PIPEDA, for an organization to place language into a contract of adhesion that has the effect of undermining an individual's *Charter* rights.

This position is strengthened through reference to section 4.3.3 of Schedule I to *PIPEDA* reads: "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes." (emphasis added) There is no need to ask individuals to "consent" to the sharing of their information with state authorities. Not only is it unnecessary for the purposes of accessing the

[8] Lisa M. Austin, "Towards a Public Law of Privacy: Meeting the Big Data Challenge" (2015) 71 Supreme Court Law Review (2d) 527.

[9] See for example: Shaw, 'Privacy Policy' s. 3.4.1 http://www.shaw.ca/privacy-policy/; Rogers 'Terms of Service, Acceptable Use Policy and Privacy Policy' at s.8 "Your Privacy" https://www.rogers.com/cms/pdf/en/Rogers-Terms-of-Service-Acceptable-Use-Policy-and-Privacy-Policy.pdf; and Telus "Our privacy commitment to you" http://about.telus.com/community/english/privacy.

[10] 2014 BCCA 319.

organization's products and services, section 7 of *PIPEDA* already has provisions for lawful access *without* consent.

Though some might argue that some personal information collected by private organizations does not attract a reasonable expectation of privacy and therefore does not require *Charter* protection, it should not be left to the discretion of private organizations to determine. This is especially true given what we know about the potentially revelatory nature of metadata. Private organizations should not have the discretion to define what is 'personal information' requiring a warrant through private contracts such as service agreements; this has the result of avoiding judicial scrutiny of state lawful access practices by diminishing an individual's reasonable expectation of privacy.

Part II Lawful access in practice

1) Recent jurisprudence on service contracts under PIPEDA: R v Ward and R v Spencer

In *R v Ward*,[11] the RCMP requested that Bell Sympatico voluntarily disclose the subscriber information affiliated with three IP addresses at specific points in time. The warrantless request was made pursuant to a child pornography investigation and was made "in accordance with" s.7(3)(c.1)(ii) of *PIPEDA*. The Ontario Court of Appeal found that Bell's service contract reduced the reasonable expectation of privacy by indicating a willingness to cooperate with authorities in criminal investigations, in addition to a policy of treating use of their services for child pornography as a breach of contract.[12] Though other factors were also considered, the contractual terms weighed heavily in the analysis.

Due to the reduced reasonable expectation of privacy, the court never examined whether police had the lawful authority required by *PIPEDA* to request voluntary disclosure. The implication of the ruling was that private organizations could reduce constitutional privacy rights of anyone using their goods or services, and that state requests for user information from those companies would evade *Charter* scrutiny altogether.

This troubling issue was somewhat resolved in *R v Spencer*,[13] in which Shaw voluntarily disclosed information that ultimately led to child pornography charges pursuant to a request made under s. 7(3)(c.1)(ii) of *PIPEDA*. The Supreme Court of Canada ruled that law enforcement authorities have no lawful authority to ask ISPs for subscriber information without a warrant. However, the specific relationship of contractual provisions to constitutional privacy rights was not clarified in that case, leaving open the possibility of warrantless access on different facts.

The key differences between *Ward* and *Spencer* lay in the different characterizations of the nature of the disclosed information and the effect of the statutory and contractual framework. The requested information was found to be more than simply a name and address, and was described as "the identity of a subscriber whose Internet connection is linked to a particular, monitored Internet activity",[14] which was found to

[11] 2012 ONCA 660 [*Ward*].
[12] *Ibid* at paras 107-108.
[13] 2014 SCC 43 [*Spencer*]
[14] *Ibid* at para 35.

engage a high level of privacy. The contractual and statutory context was found to be at best "uncertain" and therefore not determinative of the reasonable expectation of privacy.[15]

Ultimately the Court found that the requirement under s. 7(3)(c.1)(ii) of *PIPEDA* that a government institution identify its 'lawful authority' to request information meant that *PIPEDA* itself does not grant such lawful authority and does not lessen a reasonable expectation of privacy. Given that *PIPEDA* is meant to protect personal information and allows disclosure without consent only as an exception, they found a subscriber would have a reasonable expectation that a warrantless police request "would not trigger an obligation to disclose personal information or defeat *PIPEDA's* general prohibition on the disclosure of personal information without consent."[16]

The Supreme Court then determined that the manner in which the police obtained the subscriber information constituted an unreasonable search under section 8, as it was done without prior judicial authorization.

2) The aftermath of Ward and Spencer

The most important effect of *Spencer* on informational privacy is that telecom companies and ISPs no longer voluntarily disclose subscriber information in the absence of a warrant or court order. This is reflected in the annual transparency reports of several telecom companies, in which the number of voluntary disclosures of information to law enforcement authorities has dropped to zero.[17]

These rulings and the *Charter* dimensions of lawful access more generally, are crucial in the current context. Private organizations are increasingly being enlisted by state authorities as sources of information for investigations. In 2015 alone Telus reported receiving approximately 4500 separate court orders and subpoenas requiring the production of subscriber information.[18] These numbers do not accurately reflect the total number of individuals affected, as a single production order can involve records from hundreds or even thousands of people. Rogers, whose annual report breaks down disclosure by number of subscribers affected, recorded orders for information affecting a total of 86,328 subscribers in 2015.[19] The year before, a briefing note to the federal minister for public safety indicated that "Canadian police estimate that at least one form of lawful access request is made by government agencies to TSP [telecom service providers] in about 80-95 per cent of all investigations today".[20]

Unfortunately, the *Spencer* decision missed an opportunity to state that private organizations cannot require individuals to accept a reduction in their reasonable expectation of privacy in exchange for service.

---

[15] *Ibid* at paras 54-60.
[16] *Ibid* at para 62.
[17] See for example: Rogers Communications transparency report (2015) (http://about.rogers.com/about/helping-our-customers/transparency-report); Telus transparency report (2015) (https://sustainability.telus.com/en/business-operations/transparency-report/).
[18] See Telus Transparency report (2015), *supra* note 16.
[19] Rogers Communications, 'Breakdown of 2015 Requests,': http://about.rogers.com/about/helping-our-customers/transparency-report/breakdown-of-2015-requests.
[20] Amber Hildebrandt, 'Police asked telcos for client data in over 80% of criminal probes,' *CBC News*, (April 10, 2015): http://www.cbc.ca/news/technology/police-asked-telcos-for-client-data-in-over-80-of-criminal-probes-1.3025055.

Spencer leaves open the possibility that less ambiguous contractual terms might have been more determinative of the privacy right engaged. This result is antithetical to *Charter* rights, which cannot simply be contracted away, and to the purposes of *PIPEDA*. The objective of *PIPEDA* is to protect individual privacy by balancing it against the needs of private organizations to collect and use information. It is not intended to give organizations the means to tip the balance in their own favour by changing their service agreements and broadening the circumstances under which they collect, use or disclose information.

Spencer also highlights a central problem with the consent model. Schedule I of *PIPEDA* requires that for meaningful consent to use or disclosure of information to be meaningful, "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed."[21] Yet in *Spencer* a close analysis of the contractual provisions left the court uncertain as to what kind of disclosure policy the individual had consented to.[22] This is illustrative of how individuals are often faced with service contracts that potentially restrict their constitutional privacy rights in a manner they cannot reasonably anticipate or understand.

3) Tower dump records and reasonableness – R v Rogers Communications Partnership[23]

In addition to being faced with thousands of warrants and court orders annually, private organizations ae also being given the responsibility of determining whether or not those orders are reasonable. The recent ruling in *Rogers Communications* illustrates this. In that case, police obtained tower dump production orders for several towers against both Rogers and Telus. The orders required vast amounts of information, including the name and address of every subscriber communicating through the specified towers, the name and address of the person receiving that communication, and the billing information of the affected subscribers. Telus estimated it would be forced to disclose information for 9000 subscribers in order to comply. Rogers estimated it would need to produce roughly 200,000 records detailing information on 34,000 subscribers.[24] The information requested was sought in relation to the investigation of a string of bank robberies.[25]

The Superior Court concluded that the production orders went far beyond what was reasonably necessary for the investigation being conducted for the following reasons:

"For example, the Production Orders:

a) required production of information relating not only to the cell phone subscriber proximate to the crime scene but also the personal information and location of the other party to the call who may have been hundreds or thousands of miles removed from the crime scene;
b) required production of bank and credit card information which, if it had any relevance at all in locating an individual, could have been sought in a follow-up application for a small number of actual suspects …; and

[21] *PIPEDA*, Schedule I, s 4.3.2
[22] *Spencer, supra* note 12 at paras 56-60.
[23] 2016 ONSC 70 [*Rogers Communications*].
[24] *Ibid* at paras 6-7.
[25] *R v Rogers Communications Partnership*, 2014 ONSC 3853 [*Rogers Communications, 2014]*.

c) required production of personal information pertaining to over 40,000 subscribers when all the police were really interested in was information … listing the few individuals, if any, utilizing a cell phone proximate to more than one robbery location."[26]

While the Superior Court did take the opportunity to establish guidelines for the formulation of *Charter*-compliant production orders,[27] it also placed a significant burden on private organizations for assessing the reasonableness of such orders. The Court pointed out that law enforcement and judicial authorities "will only have a very general and perhaps inaccurate conception of how much personal information will be captured by a particular production order".[28] The Court found that this situation is remedied by the fact that anyone who wishes to oppose a production order can request a variance or exemption under s. 487.0193 of the *Criminal Code*.[29]

As the Ontario Court of Appeal held in *Ward*, an organization's disclosure obligations under s.7 of *PIPEDA* are conditioned by their "reasonableness" obligation under s.5(3). If we put this together with the Superior Court's comments in the *Rogers* decision that service providers are often best-placed to challenge overbroad orders then one could argue that complying with an overbroad order, and not having policies and practices in place to determine whether an order is overbroad, is a violation of s.5(3).

Finally, an issue that was only briefly touched upon in *Rogers Communication* is the fact that the production orders for the tower dump records did not specify how the disclosed data would be retained, used or disclosed by police.[30] *PIPEDA* cannot be said to provide constitutionally effective protection of individual privacy rights by regulating the collection, use and disclosure of data by private organizations when those organizations can disclose personal information to state agents who have not indicated how they will safeguard the information.

PART III Conclusions and recommendations

All of the above illustrates that while *PIPEDA* is quasi-constitutional legislation,[31] it is not itself sufficiently protective of constitutional privacy rights. Its purpose is to balance the informational privacy rights of individuals with "the need of organizations to collect, use or disclose personal information".[32] It neither anticipates nor provides for the balancing of those same informational privacy rights against the law enforcement and national security priorities of the state. The result is that private organizations – in particular, telecom companies and Internet service providers – are increasingly in the position of being responsible for protecting the constitutional rights of their customers against state authorities when faced with requests for voluntary disclosures of information or potentially unreasonable production orders.

---

[26] *Rogers Communications*, *supra* note 22, at para 42.
[27] *Ibid* at para 65.
[28] *Ibid* at para 56.
[29] *Ibid* at para 57.
[30] *Ibid* at paras 51 and 59-60.
[31] *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62, at para 22.
[32] *PIPEDA*, s.3.

As the body responsible for reviewing *PIPEDA* compliance, the Office of the Privacy Commissioner (OPC) has a constitutional role in ensuring that individual privacy rights are protected against unlawful access requests or disclosures.

The OPC should be proactively involved in reviewing both the practices of organizations in complying with lawful access requests and the related language in their service agreements and terms of use. It is not enough for the OPC to simply wait for individual complaints to be made before launching an investigation. Given the ubiquity of lawful access requests and the relatively rare cases in which an individual becomes aware of problematic disclosures of information, a reactive approach will potentially allow permissive disclosure practices that raise *Charter* concerns to continue for extended periods of time. By only examining individual complaints, the reactive model also runs the risk of failing to recognize systemic flaws in a private organization's privacy regime.

Recommendation 1: The disclosure of personal information for law enforcement, investigative or national security purposes should be subject to review that reflects the protection of s.8 Charter rights and not simply be reviewed on a reasonableness or necessity standard.

S.5(3) as it currently stands provides only for a reasonableness test akin to the standard under s.1 of the *Charter*, which is inherently a justification test. This provides inadequate protection to constitutional privacy rights as it bypasses the question of whether a constitutional privacy right was at stake and whether state access to the information was 'unreasonable search and seizure'.

In order for s.5(3) to incorporate the required s.8 *Charter* scrutiny when personal information is disclosed for law enforcement, investigative or national security purposes, it should be read to include the following principles:

1) disclosure for law enforcement, investigative or national security purposes of any personal information is not reasonable under s.5(3) without a warrant or explicit statutory requirement;
2) disclosure under a warrant that is constitutionally defective (as in excessive "tower dump" cases) is not reasonable, and;
3) the inclusion in service or user agreements of "consent" to sharing for law enforcement, investigative or national security purposes in circumstances that offer less protection than requirements (1) and (2) is not reasonable.

In this reading, consent to the disclosure of personal information is invalid where that information is disclosed to law enforcement or state authorities acting without a warrant or explicit statutory requirement, or with a constitutionally defective warrant. To use the example from *Rogers Communications*, it is not reasonable to expect an individual will have consented to the disclosure of their raw transmission data and complete subscriber and billing information when, as pointed out by the Court, a report detailing which few phone numbers were in use near several of the robberies would have satisfied the purpose of the warrant.

This means that under ss. 5(3) and 6.1 there is an obligation to ensure that business practices do not undermine the fundamental rights of customers. This obligation extends both to practices in obtaining

consent for the collection, use and disclosure of personal information and to practices in dealing with requests and orders from state authorities.

Recommendation 2: The Office of the Privacy Commissioner should take a more proactive role in PIPEDA oversight.

For the OPC to be effective as an oversight body under *PIPEDA* it must be more proactive in ensuring that the informational practices of private organizations are *PIPEDA*-compliant. A common theme running through *Ward*, *Spencer* and *Rogers Communications* is that none of the subscribers whose information was disclosed found out about the lawful access requests until they were arrested or the organization itself contested the production order.

Relying on an individual complaint-based model runs the risk that lawful access practices that are problematic from a *Charter* perspective will persist by virtue of the fact that they have not come to the attention of the individuals affected, state authorities or the courts. Private organizations will have little to no incentive to ensure their user agreements guarantee meaningful, valid consent or that their disclosure practices are in keeping with that consent – rather than occurring as an exception to consent – if these standards are unlikely to be enforced.

OPC oversight should take the form of regular review of user agreements and privacy policies to ensure they are sufficiently protective of constitutional privacy rights. These reviews should include – or possibly be combined with random audits of – policies and procedures for the handling of and compliance with warrants and production orders. The ability of private organizations to contest unreasonable warrants is not on its own sufficient protection. Even where private organizations are willing to undertake the effort of contesting warrants, and even assuming they are adequately placed to assess the reasonableness of such warrants, they should be subject to accountability measures surrounding these practices.

This kind of proactive investigation is already within the OPC's mandate.[33] Yet in reviewing Commissioner-initiated investigations over the last five years, the Asper Centre found only eight such investigations into the privacy and information practices of private companies, of which the three most recent investigations were all prompted by public reports of breaches and non-compliant processes,[34] and were not the result of any Commissioner-led auditing of those companies. None of the eight investigations examined the practices of private organizations in disclosing information to authorities.

It is especially important that the OPC examine the practices of private organizations in disclosing to law enforcement authorities because those organizations are not under any obligation to do so themselves.

---

[33] Office of the Privacy Commissioner, 'Mandate and Mission': https://www.priv.gc.ca/au-ans/mm_e.asp.

[34] The OPC's 2014 investigation into Compu-Finder email harvesting practices was based on 'hundreds' of submissions to the CRTC's Spam Reporting Centre (see Findings at https://www.priv.gc.ca/cf-dc/2016/2016_003_0421_e.asp); their 2014 investigation into Peoples Trust information safeguarding practices was based on the voluntary reporting of a breach by that company (see Findings at https://www.priv.gc.ca/cf-dc/2015/2015_007_0413_e.asp) and; their 2013 investigation into the Bell Relevant Ads program was undertaken in response to an "unprecedented number" of public complaints to the OPC, which were amalgamated into a single OPC-initiated investigation (see Findings at https://www.priv.gc.ca/cf-dc/2014/2014_011_1007_e.asp).

While companies such as Rogers and Telus have begun reporting voluntarily, they are in the minority. If Canadians are to have any confidence in legislation such as *PIPEDA* and the OPC's ability to protect their privacy rights, they need to be seen to be protecting those rights from the outset in a proactive manner, and not simply reacting after major breaches or constitutionally defective warrants have been discovered.