bccla

BC Civil Liberties Association

MOVING TOWARD A SURVEILLANCE SOCIETY

PROPOSALS TO EXPAND "LAWFUL ACCESS" IN CANADA

bccla.org

Moving Toward a Surveillance Society –

Proposals to Expand
"Lawful Access" in Canada

Philippa Lawson

Table of Contents

I. Executive Summary

The federal government has proposed new legislation that seeks to expand "Lawful Access" powers by law enforcement agencies ("LEA"s). Although justified as necessary "modernization" and just "keeping up with criminals", the proposals are deeply problematic. They would take advantage of new technologies, new modes of communication and new social practices to significantly expand access by LEAs to the personal information of individuals. Indeed, while referred to as "Lawful Access" powers, the lawfulness of some of these powers under the *Charter of Rights and Freedoms* is questionable.

The proposed expanded LEA powers include:

- Access to "subscriber data" upon request without either prior judicial authorization or reasonable grounds to suspect criminal behaviour;
- New preservation orders, available on a low evidentiary standard;
- New preservation demands with no requirement for prior judicial authorization;
- New production orders for tracking and transmission data, available on a low evidentiary standard;
- Lower evidentiary standard for, and expanded scope of, tracking warrants;
- Expanded scope of warrants for telephone number recorders to encompass all forms of transmission data.

The increased *legal* power that these proposals would expressly grant to LEAs will be greatly enhanced by the real world context of vastly more and richer personal data now available as a result of new technologies. In a "double whammy" to individual privacy, the reforms would provide LEAs with powerful new tools by which to tap this growing source of investigational data already available for investigations and intelligence-gathering. Moreover, they would do so on the basis of lower evidentiary standards - or in the case of subscriber data, no evidentiary standards at all - thus further eroding the fragile framework of privacy protection that we have constructed to control state surveillance.

Enhancing the new LEA powers would be a requirement for telecommunications service providers ("TSP"s) to be fully intercept-capable – i.e., to configure their networks so as to facilitate authorized interceptions by law enforcement agents. In addition to removing existing technical obstacles to interception by a single agent, this new law would mandate TSPs to permit multiple simultaneous interceptions by LEAs from multiple jurisdictions. Thus, the context in which police exercise their new expanded powers would be even more amenable to state surveillance, with the corollary security risk of unauthorized access and cyber-security attacks via the new mandated "back door" for law enforcement access to private communications.

One might expect that the proposals to expand police powers would be accompanied by an oversight regime with strong measures to ensure public accountability, at least where the normal requirement for prior judicial authorization is absent. Yet, there is no proposal for meaningful oversight of warrantless access powers and only a few weak measures (e.g., internal reporting and internal audits) designed to allow for some accountability. Unlike the regime governing covert interception of private communications by state authorities, there is no requirement to account publicly for the use of powers to gather data about subscribers and/or users of telecommunications services without warrant, even though data gathered in these ways can now reveal more about an individual than may be revealed by real-time interception of private communications.

Furthermore, all of the new demands, orders and warrants may be made subject to "gag orders" and, again unlike the regime governing covert interceptions by state authorities, individuals who are subject to state surveillance via the new and expanded search powers have no right to be notified of the fact. Subjects of state surveillance under these new powers are therefore unlikely ever to know of the activity unless they are eventually charged with an offence. And if individuals are unaware of searches involving them, they will be unable to challenge such searches.

Canada is not alone in proposing to expand state surveillance powers and capacity; indeed, the Lawful Access proposals are motivated to some degree by international peer pressure and Canada's desire to ratify the *Council of Europe's Convention on Cybercrime*. But the experience of other jurisdictions that have enacted similar laws in recent years is not promising: although the new laws have contributed to an explosion of state surveillance with the inevitable accompanying misuse of powers, there is little evidence that they have actually improved state security.

Canada is in a privileged position having not yet adopted the approach of these other countries: rather than proceeding on the basis of rhetoric, we can learn from the experience elsewhere and carefully examine the evidence, weighing the costs and risks that expanded state surveillance will generate against its much less clear benefits in terms of increased security. Rather than inviting *Charter* challenges and public opposition, the government should re-examine these proposals in light of the already increased surveillance powers of LEAs and the absence of any real evidence that the proposed new powers are needed to ensure the security of Canadians.

II. Introduction

In late 2005, the federal government introduced legislation entitled the *Modernization of Investigative Techniques Act* ("MITA"; Bill C-74). The MITA would have required TSPs to ensure that their networks were capable of supporting interception by LEAs, and would have forced TSPs to hand over certain basic subscriber information upon request by police. The MITA didn't survive beyond first reading due to a general election. But in its short life, the Bill generated considerable opposition from the telecommunications industry as well as from privacy and civil liberties communities.

In June 2009, the government re-introduced remarkably similar legislation entitled the *Technical Assistance for Law Enforcement in the 21st Century Act* ("TALEA"; Bill C-47). The TALEA was accompanied this time by another bill – the *Investigative Powers for the 21st Century Act* ("IP21C"; Bill C-46) – which proposed amendments to the *Criminal Code* designed to facilitate criminal investigations in the new electronic environment. The bills again generated significant opposition from those concerned with privacy and civil liberties. Privacy Commissioners from across the country passed a resolution expressing grave concern about the proposals.[1] The Bills were referred to Committee but were never reviewed and died on the order paper when Parliament was prorogued at the end of 2009.

As expected, the legislation reappeared in substantially the same form in the next session of Parliament. The *Investigating and Preventing Criminal Electronic Communications Act* (Bill C-52) and *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act* (Bill C-51), along with a third bill (C-50) addressing what one court[2] had found to be constitutional failings of warrantless[3] interception powers, were introduced in November 2010. Once again, the Privacy Commissioners collectively responded, this time with a letter to the Deputy Minister of Public Safety, expressing their continued concerns with the proposals – in particular, the "insufficient justification for the new powers", the availability of less intrusive alternatives, the need for a more "focused, tailored approach", and the need for effective oversight.[4] Bills C-50, 51 and 52 didn't make it past first reading before another general election was called. But it is widely expected that they will be re-introduced in the near future.

---

[1] See for example "Protecting Privacy for Canadians in the 21st Century" Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials on Bills C-46 and C-47 September 9-10, 2009, St. John's, Newfoundland and Labrador. Online: <http://www.priv.gc.ca/media/nr-c/2009/res_090910_e.cfm>.

[2] *R. v. Tse*, 2008 BCSC 211(CanLII).

[3] The term "warrantless" is used in this paper to mean "without a warrant or court order".

[4] See Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the current "Lawful Access" proposals dated March 9, 2011.
Online: <http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm>.

Together, these bills are referred to as "Lawful Access" initiatives – i.e., modifications of the rules regarding lawful access by police and other LEAs to otherwise private information about citizens. In this report, we use the term "Lawful Access" to mean the legislative proposals in question (rather than the existing set of rules permitting police access to private information).

In anticipation of the bills being reintroduced and making it to the committee stage, this report provides an in-depth legal/constitutional analysis of the proposals as they last appeared. It explains the import of the proposals for fundamental rights and freedoms and assesses them in terms of citizen rights. It sets the proposals in the larger domestic and international context, briefly reviewing the experience with similar lawful access initiatives in other jurisdictions.

The report concludes that the massive expansion of state surveillance powers and capabilities that would be created by the Lawful Access proposals, along with the consequent invasions of privacy and chilling of free speech, is vastly disproportionate to any benefit that the proposals would provide in terms of crime reduction. It points out that the effect of the legal powers that these proposals would expressly grant to LEAs will be compounded by the real world context of vastly more and richer personal data already available to police as a result of modern tracking devices and new communications technologies. As a result, the adverse impact on individual privacy of the kinds of investigations that would be facilitated by these new powers is much greater than was the impact on privacy of police investigations of similar investigations using old technology. Yet the proposals are accompanied by no meaningful regime to ensure effective oversight or accountability.

After subjecting each of the main proposals to a detailed analysis under sections 8 and 1 of the *Charter*, the report concludes that some of the new powers are unlikely to survive constitutional scrutiny. Those that pass the constitutional test are questionable in any case on policy grounds because of their potential for abuse, the increased risk to security that they would cause and/or the lack of a compelling justification for them. The experience of other jurisdictions with similar legislative initiatives is reviewed, highlighting the potential for such risks to be realized.

III. The Need for Strict Controls on State Surveillance

"The vibrancy of a democracy is apparent by how wisely it navigates through those critical junctures where state action intersects with, and threatens to impinge upon, individual liberties. Nowhere do these interests collide more frequently than in the area of criminal investigation."[5]

Prior to the enactment of the *Canadian Charter of Rights and Freedoms*, LEAs in Canada had broad powers of search and seizure. "Writs of assistance" could be obtained from a judge of the Exchequer Court (now the Federal Court), without discretion to refuse, for the purpose of enforcing certain statutes.[6] Police officers armed with a writ of assistance could enter and search private homes without a search warrant specific to the investigation in question. Other legislative provisions gave police officers the right to enter any place, not just dwelling houses, to search for contraband. In general, the manner in which LEAs obtained evidence in the course of their duties was of no legal consequence, except in two specific contexts: obtaining confessions and electronic interception of private communications, which were subject to constraints under the common law and the *Criminal Code*, respectively.[7]

Not surprisingly, such warrantless search powers were abused by police. In one infamous incident involving the raid of a Fort Erie tavern in 1974, "police physically searched almost all of the 115 patrons and subjected the 35 women present to strip and body-cavity searches" in an attempt to find illicit drugs.[8] This outrageously disproportionate use of force produced a total of "six ounces of marijuana, most of which was located on the floor of the tavern as opposed to on articles of clothing or within bodily cavities".[9]

Consistent with the growing societal intolerance of such state intrusions, the *Canadian Charter of Rights and Freedoms* was entrenched as part of the Canadian constitution, and included a "guarantee of protection against unreasonable search and seizure" by the state.[10] This was a turning point in Canadian legal history, as it resulted in the striking down of writs of assistance

---

[5] *R v. Mann,* 2004 SCC 52 (CanLII), paras. 15-16.

[6] *Narcotics Control Act,* R.S.C. 1970, c. N-1, s.10(3); *Food and Drug Act,* R.S.C. 1970, c. F-27, s. 37(1)(a); *Customs Act,* R.S.C. 1970, c. C-40, s. 145.

[7] Hon. Marc Rosenberg, "Twenty-Five Years Later: The Impact of the *Canadian Charter of Rights and Freedoms* on the Criminal Law", *Supreme Court Law Review*, 2nd Series, vol. 45 (Markham, ON: LexisNexis Canada, 2009). See also James Stribopoulos, "Has the Charter Been for Crime Control? Reflecting on 25 Years of Constitutional Criminal Procedure in Canada", in Margaret Beare, ed., *Honouring Social Justice: Honouring Dianne Martin* (Toronto: UofT Press, 2008), ch. 14.

[8] *Id*.

[9] Referenced in Hon. Marc Rosenberg (n. 7). See also A. Borovoy, *When Freedoms Collide: The Case for Our Civil Liberties* (Toronto: T.H. Best Printing, 1988), at 94-95.

[10] Hon. Marc Rosenberg (n. 7).

and other broad statutory powers of warrantless search. It also prompted the development of statutory limits on state powers of surveillance.[11]

Since 1982, the Supreme Court of Canada has faced an ongoing task under s.8 of the *Charter* of balancing individual liberty rights and privacy interests with a societal interest in effective policing. In so doing, it has emphasized the importance of maintaining clear limits on state surveillance. As noted by Chief Justice Beverley McLachlin in a 2008 lecture focusing on the challenge of fighting terrorism while protecting civil liberties, the Court:

> …[takes] an approach that starts with the primacy of rights and liberties, [and] permits the state to impose limits, but only where and to the extent that the state can justify these limits as reasonable in a free and democratic society. By putting the burden on the government to justify infringements on rights in the name of the broader public good, Canadian law palliates the ever-present danger that rights and liberties will be eroded in the name of fighting terrorism.[12]

The Court has made numerous statements about the need for strict constraints on police surveillance. In *R. v. Tessling*, Binnie J. stated, for the Court:

> Few things are as important to our way of life as the amount of power allowed the police to invade the homes, privacy and even the bodily integrity of members of Canadian society without judicial authorization. As La Forest J. stated in R. v. Dyment, … "[t]he restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state".[13]

LaForest J. elaborated on the point, stating as follows:

> The needs of law enforcement are important, even beneficent, but there is danger when this goal is pursued with too much zeal. Given the danger to individual privacy of an easy flow of information from hospitals and others, the taking by the police of a blood sample from a doctor who had obtained it for medical purposes cannot be viewed as anything but unreasonable in the absence of compelling circumstances of pressing necessity; see *R. v. Santa* (1983), 23 M.V.R. 300, 6 C.R.R. 244 (Sask. Prov. Ct.), at p. 251. The need to follow established rules in cases like this is overwhelming. We would do well to heed the wise and eloquent words of Brandeis J. (dissenting) in *Olmstead v. United States*, 277 US 438at p. 479 (1928): "The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well - meaning but without understanding.[14]

---

[11] *Id.*

[12] Remarks of the Right Honourable Beverley McLachlin, Chief Justice of Canada; "Symons Lecture – 2008". Online: <http://www.scc-csc.gc.ca/court-cour/ju/spe-dis/bm2008-10-21-eng.asp>.

[13] 2004 SCC 67, para. 13.

[14] *R v. Dymen*t [1988] 2 SCR 417 para. 34.

In a later case, *R. v. Duarte*, Justice La Forest for the majority further described this concern as follows:

> ... the regulation of electronic surveillance protects us from a risk of a different order, i.e., not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words. The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private.
> A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in *United States v. White, supra*, put it, at p. 756: "Electronic surveillance is the greatest leveler of human privacy ever known." If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.[15]

Scholars have also addressed this issue, focusing in recent years on the challenges to individual privacy created by new technologies. Many have emphasized the importance of anonymity in allowing people to express unpopular ideas and be critical of those in power without risking retaliation or opprobrium. George Orwell's fictional world where everything people say and do is monitored, recorded and scrutinized is widely acknowledged as antithetical to democracy and fundamental freedoms; indeed, many Canadian citizens fled here from other states precisely because of such state oppression.

In an article entitled "Why Privacy Matters Even if You Have 'Nothing to Hide'",[16] American privacy law expert Daniel Solove delves further into the threats and harms of inadequately checked state surveillance. He points out that governments can aggregate seemingly innocuous bits of information about us into highly revealing profiles; that they can exclude us from knowing about and thus controlling uses of our personal information (especially in respect of national security investigations); and that the gathering of selective information about individuals often provides a distorted picture of the real person, resulting in faulty inferences.

We in Canada should not forget our own history of inappropriate state surveillance, including the "dirty tricks campaign" of the RCMP during the 1970s. This shameful operation involved break-ins, arson and theft conducted by police officers against left-leaning press and political

[15] 1990 CanLII 150 (S.C.C.), [1990] 1 S.C.R. 30, at 43-44.
[16] *The Chronicle of Higher Education* (May 15, 2011).

parties in the name of public safety. Deception (lying to the Minister) almost kept it secret until some participants admitted their actions. A public inquiry into the affair led to the transfer of the national security mandate to a new civilian agency, the Canadian Security Intelligence Service (CSIS) and the establishment of the Security Intelligence Review Committee, tasked with overseeing the operations of CSIS.[17]

State surveillance activities, enhanced by the increasing powers of new technology, create significant risks to individual privacy and the maintenance of a free and democratic society. Overly zealous law enforcement officers need to be held in check by clear limits on their actions, as well as an effective regime of oversight and accountability.

NOTE: The next section overviews case law on s.8 (privacy rights) of the Charter. To go directly to an analysis of the specific Lawful Access proposals, turn to page 27.

[17] See Mr. Justice D.C. McDonald "Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police" 1979-1981. The Commission's reports are online: <http://epe.lacbac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm>.

IV. Existing Legal Constraints on State Surveillance

The primary constraint on police powers in Canada is the *Charter of Rights and Freedoms*, section 8 of which states that **"**Everyone has the right to be secure against unreasonable search or seizure." Section 8 jurisprudence has evolved considerably in recent years to accommodate informational privacy. Also relevant in terms of limits on police powers to access private data are certain provisions of the *Criminal Code*, as well as private sector data protection legislation which places some limits on the ability of organizations to disclose such data to the police. This chapter provides an overview of constitutional and statutory constraints on electronic surveillance by the state.

Charter of Rights and Freedoms

Section 8: "Everyone has the right to be secure against unreasonable search or seizure."

The constitutional right to be free from unreasonable search and seizure applies not just to property or territorial invasions, but to a broader notion of privacy including informational privacy. As Justice Dickson noted in the first major decision interpreting s.8 of the *Charter*, *Hunter v. Southam*, as with the fourth amendment in the United States, it "protects people, not places".[18] As early as 1993, long before the ubiquity of electronic communications, Justice Sopinka noted the importance of informational privacy in the computer age, quoting from the Report of the Task Force on *Privacy and Computers*:

> In modern society, especially, retention of information about oneself is extremely important. We may for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to for the purposes for which it is divulged, must be protected.[19]

The Court has since elaborated on the right to informational privacy under s.8 in a series of decisions involving, for example, the use by police of electricity records,[20] devices to measure electricity use in the home,[21] devices to detect heat emanating from the home,[22] tracking devices installed on cars,[23] sniffer dogs,[24] and trash left for pickup.[25]

---

[18] *Hunter et al. v. Southam Inc.,* [1984] 2 SCR 145 at 159.
[19] *R. v. Plant*, [1993] 3 SCR 281 at 15.
[20] *Id*.
[21] *R. v. Gomboc*, 2010 SCC 55, [2010] 3 SCR 211.
[22] See *R. v. Tessling* (n. 13).
[23] *R. v. Wise,* 1992 1 SCR 527.

The initial test for application of s.8 hinges on whether or not the state intrusion violated a "reasonable expectation of privacy" on the part of the complainant. Only where the subject's reasonable expectation of privacy was violated will the court find that a "search" or "seizure" under s.8 has occurred. If it is determined that a reasonable expectation of privacy was violated, a further inquiry is necessary to determine whether the search in question was authorized by a reasonable law and carried out in a reasonable manner.[26] If the search is found to have been so authorized and carried out, it will not offend s.8 even if it violated the individual's reasonable expectation of privacy.

Where individuals are found to have been subjected to an unreasonable search or seizure, the next question is whether admission of the evidence gathered via the unconstitutional search/ seizure would bring the administration of justice into disrepute. If so, the evidence is to be excluded, according to s.24(2) of the *Charter*. The exclusion of evidence under s.24(2) of the *Charter* thus serves as a safeguard for accused individuals who have been made subject to unreasonable searches, as well as a strong deterrent to unreasonable searches and seizures generally.

Where the authorizing legislation itself is being challenged as unconstitutional under the *Charter*, the next step – after determining that the search powers in question violate objectively reasonable expectations of privacy – is to determine whether the legislation can nevertheless be justified under s.1 of the *Charter* as a "reasonable limit prescribed by law as can be demonstrably justified in a free and democratic society". The party seeking to uphold the limit bears the onus of justifying it, according to the test laid out in *R. v. Oakes* (see below).

Reasonable Expectation of Privacy

When assessing whether an expectation of privacy is reasonable in a given case, the court has developed a two-stage test focusing on the totality of circumstances: (1) whether the individual concerned had a subjective expectation of privacy in the subject matter of the alleged search, and (2) whether that subjective expectation was objectively reasonable.[27] In both cases, it is important to take heed of the Court's caution that "Expectation of privacy is a normative rather than a descriptive standard."[28] In other words, it should ultimately be determined by our notions of what *should* be the case, not by technology, business practices or state practices that may themselves offend privacy.

---

[24] *R. v. A.M.*, 2008 SCC 19, [2008] 1 SCR 569, *R. v. Kang-Brown,* 2008 SCC 18, [2008] 1 SCR 456.
[25] *R. v. Patrick*, 2009 SCC 17, [2009] 1 SCR 579.
[26] *R. v. Tessling* (n. 13) para. 18.
[27] *R. v. Edwards*, [1996] 1 SCR 128 para. 45.
[28] *R. v. Patrick* (n. 25), para. 42.

Subjective Expectation of Privacy

The test for subjective expectation of privacy is a "low hurdle and individuals are presumed to have a subjective expectation of privacy regarding information about activities within the home".[29] While "a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public, or to a section of the public, or abandons in a public place",[30] personal information not so exposed or abandoned logically attracts a subjective expectation of privacy on the part of the individual to whom it pertains. This conclusion is buttressed by the existence of comprehensive data protection legislation covering both public and private sectors across Canada.

Moreover, the Supreme Court has noted that the absence of a subjective expectation of privacy,

> …should not be used too quickly to undermine the protection afforded by s.8 to the values of a free and democratic society. In an age of expanding means for snooping readily available on the retail market, ordinary people may come to fear (with or without justification) that their telephones are wiretapped or their private correspondence is being read.... Suggestions that a diminished *subjective* expectation of privacy should automatically result in a lowering of constitutional protection should therefore be opposed.[31]

Where legislation itself is being challenged as unconstitutional under s.8, the existence of a subjective expectation of privacy is inapplicable, since there are many potential subjects in question each of whom may have a different subjective expectation. The key inquiry in such cases, therefore, is into whether or not there is an *objectively* reasonable expectation of privacy in the subject-matter of the investigatory power being challenged.

Objectively Reasonable Expectation of Privacy

The objective reasonableness of an expectation of privacy in information must take into account the "totality of the circumstances" of each particular case.[32] It will depend on numerous factors, including the nature and quality of the information gathered as well as the circumstances of the gathering.

[29] *R. v. Gomboc* (n. 21), para. 117.
[30] *Tessling* (n. 13), para. 40.
[31] *Tessling* (n. 13), para. 42.
[32] *R. v. Patrick* (n. 25), paras. 26-27.

Nature of the Information

It is well established that "information which tends to reveal intimate details about a person's lifestyle and personal choices" or that constitutes a "biographical core of personal information" will attract a reasonable expectation of privacy.[33] But as Binnie J. explained in *R. v. A.M.*,

> Not all information that fails to meet the "biographical core of personal information" test is ... open to the police. Wiretaps target electrical signals that emanate from a home; yet it has been held that such communications are private whether or not they disclose core "biographical" information. ... The privacy of such communications is accepted because they are reasonably intended by their maker to be private...[34]

In the context of sniffer dogs, the Court has found that s.8 protects "specific and meaningful information intended to be private and concealed in an enclosed space in which the accused had a continuing expectation of privacy".[35] What matters is "the significance and quality of the information obtained about concealed contents, whether such contents are in a suspect's belongings or carried on his or her person."[36]

Circumstances of the Information Gathering

As noted above, the totality of circumstances must be considered in each case. Relevant circumstances include:

- the place where the alleged "search" occurred;
- whether the informational content of the subject matter was in public view;
- whether the informational content of the subject matter had been abandoned;
- whether such information was already in the hands of third parties and if so, whether it was subject to an obligation of confidentiality;
- whether the police technique was intrusive in relation to the privacy interest; and
- whether the use of this evidence gathering technique was itself objectively unreasonable.[37]

[33] *R. v. Plant* (n. 19).
[34] Binnie in *R. v. A.M.*, (n. 24), para. 68.
[35] *Id*. para.67.
[36] Binnie J. in *R. v. Kang-Brown*, see 24, *supra* para. 58.
[37] *R. v. Patrick* (n. 25), para. 27.

If it can be said that the privacy interest had been abandoned or waived, for example through failure to take measures to protect the confidentiality of the information where such measures were available, the Court will find against a reasonable expectation of privacy.[38]

Whether the complainant had notice that the information could be shared with police for law enforcement purposes is clearly relevant. However, the effectiveness of such notice is also relevant. In *R. v. Gomboc,* the Court was split as to the weight to be given to the existence of a public regulation stating that the utility could share customer data with police and allowing customers to request confidentiality. Four of the nine judges found that the regulation was but one of many factors to consider, while three found it determinative (since the complainant had failed to exercise his right to request confidentiality). The remaining two (dissenting) judges found that the regulation had no effect on reasonable expectations of privacy because:

> The average consumer signing up for electricity cannot be expected to be aware of the details of a complex regulatory scheme – the vast majority of which applies to the companies providing services, and not to the consumers themselves – which permits the utility company to pass information on electricity usage to the police, especially when a presumption of awareness operates to, in effect, narrow the consumer's constitutional rights.[39]

Similarly, the terms of service as between a complainant and the party who shared the complainant's information with the police is relevant. While the Supreme Court of Canada has yet to rule on this specific issue, it has been the focus of a number of lower court cases. In general, courts have held that clear terms permitting a telecommunications service provider to share customer information with the police in circumstances that include those in question will destroy any objectively reasonable expectation that such information will not be so shared.[40] Cases in which a reasonable expectation of privacy has been found tend to turn on an absence of evidence regarding the customer agreement, or terms that do not clearly cover the circumstance in question.[41]

Requirement for Prior Judicial Authorization

Prior judicial authorization, where feasible, is a precondition for a constitutionally valid search.[42] After repeating that the purpose of s. 8 of the *Charter* was to protect individuals against unjustified state intrusion, Dickson J. stated at p. 160:

---

[38] *R. v. Gomboc* (n. 21), paras. 108 and 118.
[39] *Id*. per McLachlin C.J. and Fish J, para. 139.
[40] *R. v. McNeice*, 2010 BCSC 1544; *R. v. Brousseau,* 2010 ONSC 6753; *R. v. Ward*, 2008 ONCJ 355; *R. v. Friers*, 2008 ONCJ 740; *R. v. Spencer*, 2009 SKQB 341; *R. v. Wilson*, [2009] O.J. No. 1067; R. v. Vasic, [2009] O.J. No. 685.
[41] *R. v. Cuttell*, 2009 ONCJ 471; *R. v. Kwok*, [2008] O.J. No. 2414.
[42] *Hunter v. Southam* (n. 18), at 160-161.

> That purpose requires a means of preventing unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in the first place. This, in my view, can only be accomplished by a system of prior authorization, not one of subsequent validation.[43]
> [emphasis in original.]

Explaining this requirement further, Dickson J. stated:

> The purpose of a requirement of prior authorization is to provide an opportunity, before the event, for the conflicting interests of the state and the individual to be assessed, so that the individual's right to privacy will be breached only where the appropriate standard has been met, and the interests of the state are thus demonstrably superior. For such an authorization procedure to be meaningful it is necessary for the person authorizing the search to be able to assess the evidence as to whether that standard has been met, in an entirely neutral and impartial manner.[44]

LaForest J. added to this reasoning in a later case involving s.8:

> ... if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. This is inherent in the notion of being secure against unreasonable searches and seizures. Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated. This is especially true of law enforcement, which involves the freedom of the subject.[45]

In general, where no circumstances exist which make the obtaining of a warrant[46] to search an office impracticable, and where the obtaining of a warrant would not impede effective law enforcement, a warrantless search cannot be justified and does not meet the constitutional standard of reasonableness.[47]

However, referring to post-*Southam* Supreme Court decisions finding that prior authorization is not required for customs searches at border crossings[48] or searches by school authorities,[49] Binnie J. has noted that the although the presumptive requirement for prior authorization remains, "the jurisprudence thus accepts a measure of flexibility when the demands of reasonableness require".[50]

---

[43] *Id*.
[44] *Id*. at 161-2.
[45] *R. v. Dyment* (n. 14), para. 23.
[46] The term "warrant" is used here and elsewhere in the paper to include production orders and other forms of legal authorization for searches.
[47] *R. v. Rao* (1984), 12 C.C.C. (3d) 97 (Ont. C.A.); leave to appeal refused ([1984] S.C.C.A. No. 107).
[48] *R. v. Simmons*, 1988 CanLII 12 (SCC), [1988] 2 S.C.R. 495, at 528.
[49] *R. v. M. (M.R.)*, 1998 CanLII 770 (SCC), [1998] 3 S.C.R. 393.
[50] *R. v. Kang-Brown* (n. 24), para. 59.

Standard for granting search warrants

The standard for granting search warrants and production orders is critical insofar as a weaker standard is more likely to encourage the "fishing expeditions" that would be deterred by a stronger standard. In *Southam,* the Court held that prior authorization for searches and seizures should bebased on a standard of belief, not suspicion. In the words of Dickson J.,

> ...The purpose of an objective criterion for granting prior authorization to conduct a search or seizure is to provide a consistent standard for identifying the point at which the interests of the state in such intrusions come to prevail over the interests of the individual in resisting them. To associate it with an applicant's reasonable belief that relevant evidence may be uncovered by the search, would be to define the proper standard as the possibility of finding evidence. This is a very low standard which would validate intrusion on the basis of suspicion, and authorize fishing expeditions of considerable latitude. It would tip the balance strongly in favour of the state and limit the right of the individual to resist, to only the most egregious intrusions. I do not believe that this is a proper standard for securing the right to be free from unreasonable search and seizure.[51]

Anglo-Canadian legal and political traditions point to a higher standard. The common law required evidence on oath which gave "strong reason to believe" that stolen goods were concealed in the place to be searched, before a warrant would issue. Similarly, section 487 of the *Criminal Code* authorizes a warrant only upon oath that there are "reasonable grounds to believe" that there is evidence of an offence in the place to be searched.

In *Hunter v Southam Inc*., the Court set the following standard:

> The state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion. History has confirmed the appropriateness of this requirement as the threshold for subordinating the expectation of privacy to the needs of law enforcement. Where the state's interest is not simply law enforcement as, for instance, where state security is involved, or where the individual's interest is not simply his expectation of privacy as, for instance, when the search threatens his bodily integrity, the relevant standard might well be a different one.[52]

[51] *Hunter et al. v. Southam Inc.* (n. 18), at 167.
[52] *Hunter et al. v. Southam Inc.* (n. 18), at 167-168.

The applicability of this standard was confirmed by the Supreme Court in a 1992 case involving the constitutionality of a statutory provision authorizing search and seizure of records relating to income tax:

> Section 231.3(3)(*b*) [of the Income Tax Act], requiring the authorizing judge to be satisfied that a document or thing which "may afford evidence" is "likely to be found", does not water down the minimum constitutional standard for the probability that the search will unearth evidence. The need to protect individuals against unreasonable searches in the form of "fishing expeditions" by the state has been recognized. A standard of credibly based probability rather than mere suspicion must be applied in determining when an individual's interest in privacy is subordinate to the needs of law enforcement.[53]

In recent years, the Court has held that the application of a lower evidentiary standard for authorizing or proceeding with a search is acceptable in certain circumstances if prescribed by legislation that can be reasonably and demonstrably justified in a free and democratic society.[54] Indeed, some Supreme Court judges have explicitly encouraged the adoption of such legislated standards in the context of tracking devices. As Cory J. stated in *R. v. Wise:*

> I agree with my colleague that it would be preferable if the installation of tracking devices and the subsequent monitoring of vehicles were controlled by legislation. I would also agree that this is a less intrusive means of surveillance than electronic audio or video surveillance. Accordingly, a lower standard such as a "solid ground" for suspicion would be a basis for obtaining an authorization from an independent authority, such as a justice of the peace, to install a device and monitor the movements of a vehicle.[55]

LaForest, J., dissenting from Cory J. in the result, agreed that lower evidentiary standards might be appropriate in certain cases but emphasized the need for full justification:

> Given the somewhat less intrusive nature of this means of surveillance, if properly controlled, than electronic audio or video surveillance, a case might be made for empowering a judicial officer in certain circumstances to accept a somewhat lower standard, such as the "solid ground" for suspicion which the peace officers claimed here, <u>if it can be established that such a power is necessary for the control of certain types of dangerous or pernicious crimes...Still this should not be permissible in the absence of cogent reasons</u>.[56] (emphasis added)

A lower evidentiary standard may be acceptable even where not prescribed by legislation. While a strong minority of judges in the 2008 “sniffer dog” cases refused to apply a

---

[53] *Baron v. Canada* [1993] 1 SCR 416.
[54] See *R. v. Wise, R. v. A.M.* and *R. v. Kang-Brown* (n. 23 and 24).
See also *R. v. Briggs,* 2001 CanLII 24113 (ONCA).
[55] *R. v Wise* (n. 23), para. 106.
[56] *Id.* para. 84.

suspicion-based standard in the absence of a legislative regime prescribing it, a majority of judges would have done so as a matter of common law in that case, given the "minimal intrusion, contraband-specific nature and pinpoint accuracy of a sniff executed by a trained and well-handled dog".[57] As these judges pointed out, the Court has applied a lower, pre-*Charter* common law test for state intrusion in some s.8 cases, notably those involving forced entry in response to a 911 call,[58] bodily searches incidental to an arrest[59] and investigative detention[60] without warrant. That test has been articulated by the Court as follows:

> The interference with liberty must be necessary for the carrying out of the particular police duty and it must be reasonable, having regard to the nature of the liberty interfered with and the importance of the public purpose served by the interference.[61]

In a recent decision involving the monitoring of electricity usage flowing into a home by way of a special device, the Chief Justice and Fish J., dissenting from the majority by finding that such police surveillance did invade the accused's reasonable expectation of privacy, then went on and applied the common law test for whether such a state intrusion was authorized by law. Finding that the warrantless use of the device by the police failed the second branch of the common law test, they reasoned that:

> This is not a case like *Kang-Brown* where police used a sniffer dog to detect drugs in the bag of a suspicious-looking person at a bus station. A police "stop and search", by virtue of its exigent nature, provides a more compelling reason for expanding common law police powers than a situation like the present where a warrant can be obtained in a timely fashion with appropriate grounds.[62]

Thus, common law does not permit state agents to forego the requirement for prior authorization except in exigent circumstances. The Supreme Court has yet to rule on whether a statutory provision permitting warrantless searches in non-exigent circumstances would survive

---

[57] Binnie and McLachlin JJ., in *R. v. Kang-Brown*, (n. 24), para. 58.
[58] *R. v. Godoy*, [1999] 1 S.C.R. 311.
[59] *Cloutier v. Langlois*, [1990] 1 S.C.R. 158.
[60] *R. v. Mann*, 2004 SCC 52, [2004] 3 SCR 59. Under the ancillary police powers doctrine articulated in R. *v. Waterfield*, [1963] 3 All E.R. 659 (C.C.A.), a search will be found to have been authorized by law if (1) it "fell within the general scope of the duties of a police officer under statute or common law", and (2) the "interference with liberty [was] necessary for the carrying out of the particular police duty and … [was] reasonable, having regard to the nature of the liberty interfered with and the importance of the public purpose served by the interference": *Dedman v. The Queen*, 1985 CanLII 41 (SCC), [1985] 2 S.C.R. 2, at paras. 68 and 69.
[61] *Id. Dedman v. The Queen*, para. 69.
[62] *R. v. Gomboc* (n. 21), para. 145.

constitutional challenge,[63] or on the constitutionality of legislation applying the lower suspicion-based standard.[64]

Agents of the State

Police cannot avoid the application of the *Charter* by doing indirectly what they cannot do directly. In this respect, courts have developed a test for determining when a private party is acting as an agent of the state. This test, first articulated by the Supreme Court of Canada in *R. v. Broyles,*[65]a case in which a private citizen was used by police to record a conversation with an accused in a jail cell, is as follows: "would the exchange between the accused and the informer have taken place, in the form and manner in which it did take place, but for the intervention of the state or its agents?"[66]

In subsequent cases applying that test, the Court has found that mere co-operation between a vice-principal of a school and the police was insufficient to establish that the vice-principal's search of a student was conducted any differently due to police intervention, or that the vice-principal was a police agent.[67] Security guards who acted independently in initiating a search of a bus depot locker, were found not to be acting as state agents, as their relationship with the police developed only after that search.[68] In a case involving a blood sample obtained by a doctor, the Supreme Court acknowledged that there are some circumstances where a doctor clearly acts as an agent of the state. But where the sample is not taken pursuant to the *Criminal Code*, or at the request of the police, there is no agency relationship for the purposes of the *Charter*.[69]

Courts of Appeal decisions shed further light on what turns voluntary private action into cooperation amounting to state agency. In a case involving Internet Service Provider ("ISP") disclosure of an accused's e-mail to the police, the Alberta Court of Appeal held that the ISP was not acting as an agent of the state prior to its contact with police because "[a]t that point, the ISP was simply performing a routine repair of the appellant's electronic mailbox at his request," but that the ISP "was acting as an agent of the state when it forwarded a copy of the message to the police at the request of the police officer."[70] Where a security guard initiated an inquiry because of her own safety concerns and her private duties to the mall, she was found not to have been acting as an agent of the state when she inquired about the item in the respondent's

[63] *Her Majesty the Queen v. Yat Fung Albert Tse, et al* which is currently before the Supreme Court of Canada,
[64] The Quebec Court of Appeal has however ruled that the legislated "suspicion"-based standard for telephone number recorders in s.492.2 does not violate the constitution: see *Cody c. R.,* 2007 QCCA 1276 (CanLII).
[65] [1991] 3 S.C.R. 595, [1991] S.C.J. No. 95.
[66] *Id.* para. 24.
[67] *R. v. M* (n. 49), at 3.
[68] *R. v. Buhay*, 2003 SCC 30, [2003] 1 SCR 631 paras. 29-30.
[69] *R.* v. *Dersch*, [1993] S.C.J. No. 119 paras. 19-20.
[70] *R. v. Weir* [2001] A.J. No. 869 at paras. 9 and 11.

hands.[71] And while merely answering questions from the police about the period of time that a blood sample would be retained by the hospital does not turn a doctor/hospital into an agent of the state, retaining the blood sample beyond the normal hospital retention period upon request of the police, solely for the purpose of the police, does turn the doctor/hospital into an agent of the state.[72]

Section 1: The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

According to the test laid out by the Supreme Court of Canada in *R. v. Oakes*,[73] two requirements must be satisfied to establish that a legislated limit "of a *Charter* right" is reasonable and demonstrably justified in a free and democratic society. First, the legislative objective which the limitation is designed to promote must be of sufficient importance to warrant overriding a constitutional right. It must bear on a "pressing and substantial concern". Second, the means chosen to attain those objectives must be proportional or appropriate to the ends. The proportionality requirement has three aspects: the limiting measures must be carefully designed, or rationally connected, to the objective; they must impair the right as little as possible; and their effects must not so severely impinge upon individual or group rights that the legislative objective, albeit important, is nevertheless outweighed by the abridgement of rights.

As the Court stated in a later case, this test is ultimately concerned with "whether the benefits which accrue from the limitation are proportional to its deleterious effects".[74]

In a number of cases, the Supreme Court has found that while random spot checks by police do violate the right under s.9 of the *Charter* of drivers "not to be arbitrarily detained", they are justified under s.1 as reasonable limits, given the statistics relating to the carnage on the highways, the nature and degree of the intrusion of a random stop for the purposes of the spot check procedure, and the fact that the driving of a motor vehicle is a licensed activity subject to regulation and control in the interests of safety.[75] As stated by the Court in *R. v. Ladouceur*:

> The means chosen was proportional or appropriate to those pressing concerns. The random stop is rationally connected and carefully designed to achieve safety on the highways and impairs as little as possible the rights of the driver. It does not so severely trench on individual rights that the legislative objective is outweighed by the abridgement of the individual's rights. Indeed, stopping

[71] *R. v. Chang*, 2003 ABCA 293 (CanLII), paras. 16-18.
[72] *R. v. Lunn*, 1990 CanLII 1237 (BC CA).
[73] 1986 CanLII 46.
[74] *Thomson Newspapers Co. v. Canada (Attorney General)*, 1998 CanLII 829 (S.C.C.) para. 125.
75 *R. v. Hufsky* [1988] 1 S.C.R 621; R. v. *Ladouceur* 1990 1 SCR 1257.

> vehicles is the only way of checking a driver's licence and insurance, the mechanical fitness of a vehicle, and the sobriety of the driver.[76]

Now under appeal before the Supreme Court of Canada, a 2008 decision of Davies J. of the British Columbia Supreme Court held that s.184.4 of the *Criminal Code*, which authorizes interception of private communications without prior judicial authorization in certain circumstances, violates s.8 of the *Charter* and is not saved by s.1 because of the lack of adequate safeguards against state abuse of the provision.[77] Judge Davies enumerated the many additional safeguards applicable to interceptions under other provisions of the Code that could be applied, but have not been applied, to s.184.4 interceptions.[78] A judge of the Ontario Superior Court also found s.184.4 constitutionally wanting, but in only two respects, each of which could in his view be remedied either by severance or "by reading down".[79] Bill C-50, introduced by the government in the last session of Parliament, would have added some of the safeguards to s.184.4 that the lower courts noted were missing.

The Criminal Code

In addition to constitutional limits on state surveillance are statutory constraints (themselves subject to constitutional challenge). The *Criminal Code* sets out a regime for state intrusions on individual privacy, distinguishing between real-time interception of private communications (Part VI) and search and seizure (Part XV – ss.487ff). In general, it applies the highest standard of protection against state intrusion to real-time interception of communications and video surveillance.

Interceptions are permitted only for the purpose of investigations of those serious offences listed in s.183. In cases of interception with consent (most commonly, an informer), police must obtain prior authorization on the basis of reasonable grounds to *believe* that one of the listed offences has been or will be committed and that information concerning the offence *will be obtained* via the interception.[80] Prior authorization is not required for interceptions with consent of one party where certain other conditions apply (to prevent bodily harm[81]or in a situation of urgency[82]), but

---

[76] *Id. R*. v. *Ladouceur.*

[77] *R. v. Tse* 2008 BCSC 211 (CanLII); see also *R. v. Six Accused Persons*, 2008 BCSC 212 (CanLII), a similar judgment of Davies, J.

[78] *Id.* para. 200.

[79] *R. v. Riley*, 2008 CanLII 36773 (ON SC). Dambrot J. concluded at para. 4 that "s.184.4 of the *Criminal Code* is inconsistent with the *Charter* in two respects: (1) … the availability of the extraordinary power to intercept without prior judicial approval exceeds what is reasonable within the meaning of s.8 of the *Charter* because of the overbreadth of the definition of peace officer in so far as it governs who may make use of s.184.4; and (2) the absence of an obligation to give notice to objects of interception is inconsistent with s. 8 of the *Charter.* I have further concluded that the first of these deficiencies can be remedied by severance, and the second by reading down. With these deficiencies remedied, I conclude that the overall scheme in s. 184.4 is reasonable."

[80] S. 184.2.

[81] S. 184.1(1)(b).

the party conducting the interception must nevertheless have reasonable grounds to believe that the specified conditions exist. Interceptions without consent are permitted only if a judge (not justice of the peace) is satisfied that (a) there is no other feasible, less intrusive method of obtaining the evidence (unless the investigation regards organized crime or terrorism), and (b) the interception is in the best interests of the administration of justice.[83]

Ex post facto safeguards for real-time interceptions include annual reporting requirements and a requirement to notify the subject of the interception within 90 days of the end of the authorization period.[84]

Other state powers of search and seizure, including production orders and tracking warrants, are subject to a completely different regime. They are not limited to particular serious offences. Nor do they include *ex post facto* reporting or notification requirements. Prior authorization can be obtained from a justice of the peace as opposed to a judge, and is not required in exigent circumstances.[85] Evidentiary standards vary according to the type of search or order sought. General search powers and production orders, like interceptions, require reasonable grounds to *believe* that an offence has been or will be committed and that the information to be obtained *will afford evidence respecting the offence* in question.[86]

However, tracking warrants, warrants to use telephone number recorders, and production orders for specific financial account information are all subject to a lower evidentiary standard, presumably on the basis that they represent a lesser intrusion into individual privacy.[87] In the case of tracking warrants, the justice must be satisfied that there are reasonable grounds to *suspect* that an offence has been or will be committed and that information relevant to the offence *can be obtained* through the use of the tracking device.[88] Warrants for dial number recorders and production orders for specific financial account data are both available on the basis of reasonable grounds to *suspect* that an offence has been or will be committed and that information obtained *will assist in the investigation of the offence.*[89]

Data Protection Legislation

LEAs are also indirectly limited in their data collection activities by data protection legislation, which places restrictions on the right of organizations to divulge "personal information" (defined as any information about an identifiable individual) to others without the individual's

---

[82] S. 184.4.
[83] S. 184.6.
[84] S. 185, 186, 195, 196.
[85] S. 487.11.
[86] See for example, s. 184.2(2) and (3).
[87] The constitutionality of these lower standards has not yet been put to the Supreme Court of Canada.
[88] S. 492.1(1).
[89] S. 492.2(1).

consent. Telecommunications service providers are federally regulated, and so the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") applies to them.

Under PIPEDA, TSPs are permitted to disclose personal information to LEAs if they have the individual's consent or if they are required to do so by court order, warrant or subpoena.[90] They are also permitted to disclose such information to police on their own initiative if they have reasonable grounds to believe that the information relates to an offence or if they suspect that it relates to national security.[91] Finally, they may provide personal data in response to a request by a law enforcement agency that has "identified its lawful authority to obtain the information" and has indicated either that it "suspects that the information relates to national security", or that it is requesting the information for the purpose of (a) investigating or enforcing a domestic or foreign law, or (b) administering a domestic law.[92] But unless they are required to disclose the information by court order, for example, TSPs can refuse to do so.

[90] S. 7(3)(c).
[91] S. 7(3)(d).
[92] S. 7(3)(c.1).

V. The Changing Context

Far from "Going Dark" as a result of advances in technology, the FBI and other law enforcement agencies are experiencing a boon in electronic surveillance.[93]

The *Criminal Code* provisions on interception of private communications and search and seizure were designed in the pre-internet era, when people communicated across distances largely by telephone and postal mail. The content of one's telephone communications was ephemeral (other than in exceptional circumstances), and the content of one's postal communications was unrecorded (except possibly by the sender or recipient).

The internet – and other new technologies – has changed all that. Now people communicate to an increasing extent by electronic mail, online social networking, online chat and text messaging – digital modes that automatically record not only the message but the transmission information surrounding it. We also use the internet to seek information of interest to us, to engage in transactions and to share information with others through websites and social networking sites. All of this online activity leaves a digital trail that cannot be easily hidden and that can never be fully erased. Our digital trails are stored on computer servers operated by service providers as well as on our own personal computers, where they are available for lawful (and unlawful) access.

Electronic exchange has thus superseded voice as the main way in which we communicate other than face-to-face. We now send e-mails or text messages *instead of* telephoning friends. Information that in the past was obtainable only by real-time interception is now available via much less onerous searching, long after the fact. Most of us don't give much thought to the privacy implications of these powerful new methods of communication – we simply trust that our private communications will stay out of prying hands. The same privacy interest inheres in the communication: only the mode has changed.

With digital technologies, as soon as a text or email communication takes place it is immediately stored on a server somewhere in the world that is remotely accessible by authorized third-parties. The implications of this for LEAs are enormous: no longer must an intelligence or police officer be physically proximate to the communication, wait patiently for a communication to occur, or await the delivery of physical copies of messages after they arrive in a storage location. Now authorities can remotely access communications in near-real-time;[94] close enough

[93] Centre for Democracy and Technology, "FBI Seeks New Mandates on Communications Technologies", February 24, 2011. Online at: http://www.cdt.org/policy/fbi-seeks-new-mandates-communications-technologies.

[94] Sprint and other telecommunications firms have established call centers to more quickly clear and respond to law enforcement requests (see: C. Soghoian, "8 Million Reasons for Real Surveillance Oversight" (December 1,

to when the communication take place as to provide comparable response capabilities as with a real-time communication.

Moreover, we are exchanging and exposing exponentially more information about ourselves now as a result of these electronic technologies than we did in the past. Some of this exposure is voluntary and informed – e.g., personal websites of adult professionals. Much is voluntary but uninformed – think of young people's Facebook profiles, the record of your book purchases on Amazon.com, or all those "user agreements" that you click "I agree" to without reading. And some is neither voluntary nor informed – e.g., information about us posted by others, or online communications to us from others. Regardless, the information that we leave in our digital footprints is far more extensive than was the information that we left in our voice and written communications just twenty years ago. It reveals details about our social circles, our friendships and love lives, our professional activities, our business plans, our political leanings and our religious affiliations, to mention just a few potentially sensitive topics.

In addition to the digital trails we leave online are the digital trails that we now leave in the offline context. We use automatic teller machines rather than waiting in line at the bank. We use debit and credit cards instead of cash. We store our voice mail on computers owned by the telephone company rather than on machines in our homes and offices. We use RFID-enabled access cards rather than keys to access our offices and apartments. We use Global Positioning System ("GPS") enabled mobile telephones that track our whereabouts, rather than public payphones that can't be traced to us. We use electronic road tolls rather than stopping to pay in cash. This data can reveal exactly where we went, at exactly what time, and for what purpose, from the time we rise in the morning to the time we go to bed.

Furthermore, new technologies allow businesses and others to compile these digital trails into highly revealing personal profiles at very little cost or effort. In fact, any business that does not accumulate and analyze its customer information, for its own purposes if not for the purpose of sharing with others, is now seen as wasting a valuable commercial resource. Loyalty cards are hugely popular among consumers, allowing companies to amass an ever-richer profile of each consumer. Our credit histories are collected, stored, and sold by companies we don't even know exist. An entire industry of data-brokers has emerged to capitalize on the profit to be made from mining and selling this information. The personal profiles thus compiled can reveal more about us than we ourselves appreciate.

Authorities thus now have available to them a veritable goldmine of personal data, unlike anything available to them in the past. Much of this information is publicly available, and value-added versions of it can be purchased on the open market. Investigators need only sit

---

2009). Online: <http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html>). Cloud computing providers such as Google have established Lawful Access portals that allow authorities with warrants to remotely access communications that are stored on Google servers (see: B. Schneier, "US Enables Chinese Hacking of Google" (January 23, 2010) online: <http://www.schneier.com/essay-306.html>).

at a computer to find evidence of illegal activity and begin tracing it to a suspect. Individuals often disclose intensely personal and revealing information about themselves online, under pseudonyms and usernames, assuming that their privacy is protected by a cloak of anonymity. All that is needed to complete the package is a name and address.

And vastly more information is now available to authorities when they do get permission to track individuals via GPS-enabled devices or transmission data recorders, or to obtain subscriber/user records from service providers. Telephone numbers have been replaced with transmission data that provides precise information about routing, signalling, origination and destination addresses.

Tracking devices can now be remotely activated and adjusted, enabling 24 hours a day "dragnet" surveillance at minimal cost – i.e., a complete technological replacement for physical human surveillance.

As Daniel Solove points out,

> Technology is giving the government unprecedented tools for watching people and amassing information about them - video surveillance, location tracking, data mining, wiretapping, bugging, thermal sensors, spy satellites, X-ray devices, and more. It's nearly impossible to live today without generating thousands of records about what we watch, read, buy, and do–and the government has easy access to them.[95]

The context of police access to information has thus changed dramatically, even just over the past decade. There is now far more information, and far richer information, about individuals freely available to LEAs. A similarly larger body of richer information is also now available to LEAs through interceptions, searches and production orders than was ever available in the past. At the same time, technological developments continue to further facilitate and enhance surveillance of others, authorized or not. Yet the privacy interest in such information has not changed - individuals are just more vulnerable now to privacy invasions than ever before.

Proponents of Lawful Access argue that "[l]egislation must be modernized in order to keep pace with modern communications technology and give investigators the tools they need to perform complex investigations in today's high-tech world".[96] There is indeed a need to "modernize" criminal laws to take into account these new realities. But the new reality actually makes available to police more, not less, information about us. Legislative modernization therefore needs to provide for stronger, not weaker, controls on state surveillance.

---

[95] D.J. Solove *Nothing to Hide*: *The False Tradeoff between privacy and security*, (Yale University Press, 2011), at 2.

[96] Department of Justice Canada, "Backgrounder: Investigative Powers for the 21st Century (IP21C) Act" (June 2009).

VI. The Proposals

Overview

The proposed new laws and amendments break down into two types: those enhancing the legal *powers* of police to engage in search and seizure, and those enhancing the practical *ability* of police to exercise their powers. In the latter category is the proposal to require that all telecommunications service providers be capable of facilitating interceptions by authorized government agents. The remaining proposed law reforms fall into the former category.

The proposals would make numerous changes to the statutory powers governing state access to private information in the course of law enforcement investigations. With one exception (tracking warrants for devices carried or worn by individuals), these reforms would give law enforcement agents greater powers to access information, either by expanding the scope of certain warrants, providing a means to ensure that potentially relevant information is preserved while a production order is being sought, lowering the applicable standard for obtaining certain orders and warrants, or, in the case of subscriber data as well as preservation demands, eliminating the need for prior authorization at all.

To the extent that this law reform initiative is designed to bring more clarity to the rules governing certain aspects of search and seizure, it is to be welcomed. The Supreme Court has struggled in recent years when applying the *Charter* to informational privacy in the context of rapidly changing technologies and social practices, without clear legislative standards.[97] However, it is misleading to characterize these reforms as mere clarification or "modernization" of the law – jurisprudence on the common law and constitutional validity of the proposed standards and measures is mixed, and the "modernization" that these proposals would bring about does not simply maintain existing state powers – it expands them, significantly.

Each proposal is described and analyzed below.

Mandatory Intercept Capability by Telecommunications Service Providers

Following the lead of other jurisdictions including the United States (US), United Kingdom (UK) and Australia, Canada is proposing to compel TSPs to be technically capable of intercepting communications over their networks and of providing such intercepted communications to authorized law enforcement officials.[98] TSPs would be required to isolate communications to a

[97] See, for example, *R. v. A.M.* and *R. v. Kang-Brown* (n. 24): in both cases, four of the nine judges held that legislation was required to lower the evidentiary standard for sniffer dog searches.

[98] Bill C-52, *An Act regulating telecommunications facilities to support investigations*, 3rd Sess, 40th Parl, 2010 (first reading 1 November 2010) [IPCEC], s. 6.

particular individual and to enable simultaneous interception of multiple communications as well as simultaneous interceptions by law enforcement authorities from multiple jurisdictions.[99] TSPs would be required to decrypt intercepted communications that are encrypted (or otherwise made unreadable by a TSP) if they have the means to do so.[100] TSPs would also be required to assist in testing police surveillance capabilities[101] and to disclose the names of all employees who may be involved in interceptions (and who may therefore be subject to RCMP background checks).[102] Failure to comply with these obligations would be subject to significant financial penalties.

Analysis

This proposal would not expand police *powers* as such; the same rules for authorizing interceptions would continue to apply. It would, however, significantly expand police *ability* to engage in interception of communications when they have obtained authority to do so. It can thus be expected to result in a significant increase in wiretaps by LEAs.

Although we look to legal constraints rather than technical obstacles to limit state surveillance, there is reason to be concerned about the "architecture of surveillance" that mandatory intercept capability would create. With the inevitable increase in interception as a result of this surveillance-ready infrastructure, there will be an even greater need for effective oversight and safeguards against abuse. Yet the package of proposals for increased Lawful Access includes no change to the inadequate oversight regime that currently exists.

Another serious concern with this proposal is the increased vulnerability of personal data to unauthorized access that it will create. By requiring TSPs to maintain a "back door" for law enforcement surveillance, the state is creating a heightened risk that hackers will exploit that back door for their own, possibly criminal, purposes. As IBM researcher Tom Cross noted when describing security vulnerabilities in Cisco's wiretapping architecture, these weaknesses would let a criminal "produce a request for interception that had a valid username and password, thus enabling him to get the fruits of a wiretap."[103]

[99] *Id.* s. 7(b) and (d).
[100] *Id.* s. 6(3).
[101] *Id.* s. 25.
[102] *Id.* s. 28.
[103] Susan Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (Cambridge, Mass.: The MIT Press, 2010) at 196-7.

Indeed, this is exactly what happened to Google in late 2009: Chinese hackers were able to take advantage of a system to help Google comply with state demands for data on Google users, in an apparent effort to access the Gmail accounts of Chinese human rights activists.[104]

Governments themselves may find it too tempting not to take advantage of a greater capacity to engage in real-time surveillance without proper legal authority. After the terrorist attacks of 2001, the US National Security Administration (NSA) built a surveillance infrastructure to eavesdrop on communications to and from foreign sources. A national controversy erupted after it was discovered that this surveillance program had been used to spy on domestic as well as foreign communications, contrary to US law.[105] More recently, the NSA admitted that it had "been engaged in over-collection" of domestic email messages and phone calls in the course of its foreign intelligence activities.[106]

Perhaps the most chilling example of unauthorized use of technical intercept capability is that which occurred in Greece between June 2004 and March 2005, at the time of the Greek Olympics. Using wiretapping capability that Ericsson had built into Vodafone's projects for use by governments, an unauthorized person or entity managed to wiretap more than 100 cell phones belonging to the prime minister and senior government officials.[107]

Before requiring TSPs to compromise network security by creating access points for law enforcement, there needs to be a thorough review and analysis of vulnerabilities that would be thereby created, so as to minimize the potential for unauthorized access. Before forcing these costly and undesired measures upon the private sector, the government owes a duty to Canadians to ensure that the intercept capability it is forcing on TSPs for the alleged purpose of enhancing their security will not in fact have the opposite effect of *compromising* the security of their communications.

Finally, proposals to require TSPs to configure their networks so as to facilitate state surveillance effectively deputize private actors in criminal investigations by the state. While this aspect of the proposed legislation is unlikely to be found unconstitutional,[108] it raises serious issues as to the point beyond which states should not be allowed, legislatively or otherwise, to forcibly enlist

---

[104] R. McMillan "Google attack part of widespread spying effort U.S. firms face ongoing espionage from China" January 13, 2010. Online: <http://www.computerworld.com/s/article/9144221/Google_attack_part_of_widespread_spying_effort>

[105] See NSA warrantless surveillance controversy. Online: <http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy#Overview>.

[106] E. Lichtblau and J. Risen *Officials Say U.S. Wiretaps Exceeded Law* April 15, 2009. Online: <http://www.nytimes.com/2009/04/16/us/16nsa.html?_r=1>.

[107] *Greek wiretapping case 2004–2005* online: <http://en.wikipedia.org/wiki/Greek_wiretapping_case_2004%E2%80%932005>. While US intelligence agencies have been informally identified as suspects, the identity of the perpetrators has still not been established.

[108] Mandating private organizations to act as agents of the state *per se* does not violate any constitutional right or freedom.

private actors in the conduct of what is indisputably state business. The fact that other countries have implemented similar requirements, or that Canada has agreed by treaty to do so,[109] does not make such measures appropriate in a free and democratic society.

Warrantless Access to Subscriber Data

This, the most criticized of the "Lawful Access" proposals, would require TSPs to provide specified subscriber information to designated law enforcement officers upon request, without prior judicial authorization and without any requirement for reasonable grounds.[110] While TSPs are arguably now *permitted* to disclose such information to LEAs in the absence of a warrant,[111] they can refuse to do so and apparently some do. This provision would thus expand the power of law enforcement to demand certain investigatory information from TSPs who would otherwise require a warrant before providing the requested information.

Subscriber information vulnerable to such requests would include "name, address, telephone number and electronic mail address of any subscriber to any of the service provider's telecommunications services and the Internet protocol address, mobile identification number, electronic serial number, local service provider identifier, international mobile equipment identity number and subscriber identity module card number that are associated with the subscriber's service and equipment".[112] Such information is particularly valuable insofar as it allows police to link anonymous online activity and communications with an individual name.

The proposed new power would be available to a finite number of designated law enforcement officials[113] for the purposes of performing duties or functions of a police service, the "CSIS", or the Commissioner of Competition, including for the enforcement of foreign laws.[114] The number and type of law enforcement officials who could exercise this power would thus be much fewer than the broad category of "peace officers" and "public officers" authorized to apply for search warrants and production orders under the *Criminal Code*.

But no condition beyond fulfilling a duty or function of the agency – not even suspicion of illegal activity – would be required for a designated official to demand this information. There would be no limit to the number of requests that could be made or to the type of offences for which this unprecedented investigatory power could be used.

---

[109] See Article 20 of the Council of Europe Convention on Cybercrime (ETS no. 185) Budapest, 23.XI.2001, which Canada has signed and intends to ratify once necessary legislative changes have been implemented.
[110] Bill C.52, s. 16.
[111] PIPEDA s. 7(3)(c.1). NOTE: for the sake of convenience, the term "warrant" in this section includes production orders and any other enforceable order for disclosure.
[112] S. 16 (n. 110).
[113] The greater of five or 5% of the agency's total staff: Bill C-52, s. 16(4).
[114] Bill C-52, s. 16(2).

Requests would normally have to be made in writing by designated officials only. However, in situations where a non-designated police officer believes on reasonable grounds that the information requested is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property, where the information sought directly concerns either the victim or the perpetrator, and where the officer believes on reasonable grounds that the urgency of the situation demands an immediate response, the officer would be empowered to obtain the information merely upon verbal request.[115]

While there is no "gag order" provision in the statute itself, the proposed law provides for regulations to be made "prescribing any confidentiality or security measures with which the telecommunications service provider must comply".[116] Such regulations could apply generally or to particular classes of TSPs.[117] It can therefore be expected that TSPs will be under a regulatory obligation not to disclose the existence or content of the request.

There is no provision for TSPs to challenge the warrantless demands other than by refusing to provide the requested information. Such refusals are highly unlikely given the considerable consequences to TSPs, who could be charged with an offence punishable by a fine of up to $250,000 per day of refusal.[118] Moreover, individuals whose subscriber information is disclosed to police under this provision would not be given notice after the fact (as are subjects of wiretaps[119]).

Although the proposed new law explicitly limits secondary uses of subscriber information gathered under this power, it would allow law enforcement and intelligence agents to use the information without the individual's knowledge for purposes "consistent with" the original purpose for which it was obtained.[120] In the context of intelligence, there is no real limit on information gathering – all information about a suspect is potentially relevant. Once again, there is no after-the-fact notice provision ensuring that the subscribers in question are aware, let alone consent to, such uses.

The proposal would require that each agency keep records of each request, including the duty or function under which the request was made and the relevance of the information to that duty or function. Each agency would also be required to conduct internal audits of its practices under these provisions on a regular but unspecified basis, and to report to the responsible minister about "anything arising out of the audit that in his or her opinion should be brought to the attention of that minister..."[121] The proposals also include provisions for discretionary auditing by the Office of the Privacy Commissioner of Canada (of the RCMP

[115] *Id.* s. 17.
[116] *Id.* s. 64(1)(l)(ii).
[117] *Id.* s. 64(2).
[118] *Id.* ss. 57, 61.
[119] *Criminal Code,* s. 196.
[120] Bill C-52, s. 19.
[121] *Id. s*. 20(2).

and Competition Bureau) and the Security Intelligence Review Committee (of CSIS), but such provisions are redundant given that those bodies already enjoy such audit powers.[122] There is no provision for auditing of municipal or provincial police force use of this new power.

Charter Analysis

Reasonable Expectation of Privacy in Subscriber Data

The first question in an analysis of whether this proposal is *Charter* compliant is whether the data in question (name, telephone number, addresses, IP address, etc.) attracts an objectively reasonable expectation of privacy.

This subject has never been fully addressed on appeal, with one appellate court simply commenting in *obiter* on the unsettled state of the law.[123] Lower courts have found both for[124] and against[125] a reasonable expectation of privacy in subscriber information. While the latter category of decisions is greater in number, the reasoning in such cases lacks consistency and it is therefore difficult to deduce clear principles other than regarding the significance of service agreements between subscribers and service providers.

Nature and Quality of the Information

On its face, subscriber information clearly does not reveal "intimate details about a person's lifestyle and personal choices", nor does it constitute a "biographical core of personal information". However, subscriber information is never requested by police for its intrinsic value; rather, this information is valuable to police precisely because of its link to highly personal, intimate and in many cases incriminating information that the police have already amassed. As the judge in one case reasoned:

> Once the police accessed Mr. Cuttell's name and address, they were able to link his identity to a wealth of intensely personal information. Linking his name to the shared folder under his IP address, police learned a great deal about Douglas Cuttell and his lifestyle: namely in this case, his interest in adult pornography, obscenity and child pornography, which were all revealed by his choice of shared files.[126]

[122] *Id.* ss. 20(4) and (5).
[123] *R. v. Ballendine,* 2011 BCCA 221 (CanLII), para. 74.
[124] See 44.
[125] See 43.
[126] See 44, para. 21.

None of that information in the public domain was meaningful to police until it was associated to Mr. Cuttell himself. More importantly in terms of privacy, none of that information was significant to Mr. Cuttell's privacy until it was linked to him personally. It was only once his identity was known that his privacy was invaded.

This point was made in the context of banking records in *R. v. Eddy* where the Newfoundland Supreme Court held that:

> The linkage of a name to [account] information creates at once the intimate relationship between that information and the particular individual, which is the essence of the privacy interest. I do not accept the Crown's suggestion that the mere obtaining of the name of the owner of an account about which information is already available is not deserving of protection under s.8.[127]

As some commentators have emphasized,

> The point cannot be sufficiently underscored: typical subscriber information of the sort made available under the proposed legislative scheme will become the means by which a biographical core of personal information is assembled.[128]

The value of subscriber information as a key to unlocking anonymous information already amassed (as well as troves of additional sensitive personal information) distinguishes it from other information that police seek in the context of criminal investigations. While transaction records, billing statements, utility records and other information gathered during an investigation add to each other like pieces of a puzzle, none of which is sufficient on its own to establish culpability, these kinds of personal data do not serve as a critical link to biographical core information that has already been gathered and that is often incriminating on its own – all that is needed is a name to attach to the anonymous suspect.

Moreover, the very fact that a person has used a pseudonym or otherwise concealed his or her identity in the context of online communications is clear evidence that the person considers his or her identity, in that context, to be private. Similarly, an unlisted telephone number is a clear indication of the subscriber's expectation of privacy in that number. Once linked with incriminating or otherwise sensitive information, there can be no question that non-public subscriber information constitutes "specific and meaningful information intended to be private and concealed", and thus attracts a reasonable expectation of privacy.[129]

This conclusion is further supported by the fact that data protection legislation in Canada recognizes the significant privacy value inherent in subscriber data and prohibits TSPs from

---

[127] *R. v. Eddy* [1994] N.J. No. 142 para. 175.
[128] D. Gilbert et al., "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunication Providers" 51 *Crim.L.Q.* 469 (2005-2006) at 503.
[129] See *R. v. A.M.* (n. 24), para. 67.

disclosing it to non-governmental third parties for the purpose of identifying alleged civil wrongdoers without a subpoena, warrant or court order.[130] Indeed, in civil cases involving requests for disclosure of subscriber information, typically for the purpose of defamation and copyright infringement lawsuits, courts have noted the importance of privacy in one's identifying information.[131]

There would therefore appear to be an objectively reasonable expectation of privacy in subscriber data – at least in those cases where it functions as a link to "specific and meaningful information intended to be private".[132] But the analysis of whether an objectively reasonable expectation of privacy exists must also consider the circumstances under which subscriber information would be provided to police under the proposed new regime.

Circumstances of the Information Gathering

Location is not material since the proposed new power is in the nature of a production order rather than a physical search. Nor is the technique used by police to obtain the evidence – a written request and, in exceptional circumstances, a verbal request – of any import in the privacy analysis.

It is however relevant that this information is not in public view (otherwise the police would not have had to request it from the TSP). Rather, it is a private record belonging to the TSP. Although subscribers knowingly provide this information to the TSP, they do so because they *must* in order to obtain the service; it cannot be said therefore that subscribers abandon the information when they provide it to the TSP. Indeed, the TSP is under a legal obligation to keep this information secure from unauthorized access[133] and confidential, except for specific purposes set out in legislation.[134]

The terms of the subscriber agreement are also relevant and have indeed been determinative in many cases decided to date on this issue, with lower courts remarkably consistent in their treatment of this factor. If the terms of service clearly allow for the disclosure of subscriber information to police, courts have found there can be no reasonable expectation of privacy in that

[130] PIPEDA, s. 7(3).
[131] *BMG Canada Inc. v. Doe,* 2005 FCA 193 (CanLII), *BMG Canada Inc. v. John Doe*, 2004 FC 488 (CanLII) para.37: "In keeping with the protocol or etiquette developed in the usage of the internet, some degree of privacy or confidentiality with respect to the identity of the internet protocol address of the originator of a message has significant safety value and is in keeping with what should be perceived as being good public policy".
[132] *R. v. A.M.* (n. 24), para. 67.
[133] PIPEDA, s.5(1) and Schedule 1, Principle 4.7.
[134] *Id.* s.7(3).

information.[135] In those cases where a reasonable expectation of privacy was found, evidence concerning the nature of the service agreement was either not available or not considered.[136]

Widespread as it is, this treatment of subscriber agreements fails to take into consideration the extent to which the terms of service unilaterally imposed by TSPs on subscribers constitute a voluntary "agreement" in any meaningful sense – i.e., the extent to which subscribers are made aware of the term regarding disclosure, whether subscribers have any choice in accepting this term, whether subscribers have available to them alternative service providers that do not require consent to such disclosures, and the extent to which it is reasonable to expect individuals to take such clauses into account when selecting service providers. As the dissenting Supreme Court judges in *R. v. Gomboc* noted, courts should be cautious in presuming awareness of a regulation where such presumption operates to narrow constitutional rights.[137] The same applies to presumptions of voluntariness in the context of mass market agreements.

But even if terms of service are treated as voluntary informed agreements sufficient to negate an otherwise reasonable expectation of privacy, such terms will vary among agreements and service providers. Indeed, it can be expected that some TSPs will distinguish themselves by not requiring that their subscribers agree to a term permitting disclosure to police (they do not need to obtain consent for mandated disclosures). Without knowing that the terms of the agreement in any given case provide for disclosure to police, the government cannot defend warrantless access to subscriber data on that basis.

Some courts have treated as relevant the fact that TSPs are permitted, under PIPEDA, to disclose subscriber information to LEAs upon request, as long as the agency has "identified its lawful authority to obtain the information".[138] With respect, this reasoning reflects a misunderstanding of PIPEDA. As noted by the court in *R. v. Cuttell*, PIPEDA governs private organizations, not the police.[139] While it *permits* TSPs to disclose subscriber information to government authorities with "lawful authority" to request the information, such permission in no way authorizes police to obtain subscriber data without a court order. All that PIPEDA does in this respect is to leave it up to the TSP to determine whether or not the data requested attracts a reasonable expectation of privacy and thus whether or not a warrant is required. (As noted below, this is an unrealistic approach: TSPs cannot be expected to make legal/constitutional determinations before responding to each request for subscriber data.)

The possibility that *some* subscribers will have a reasonable expectation of privacy in their name and address means that a general approach ignoring that fact will be inconsistent with the *Charter*. That is the case with the proposal in question: it is incorrectly premised on the

[135] See R. v. *McNeice, R. v. Brousseau, R. v. Ward, R. v. Friers, R. v. Spencer, R. v. Wilson, R. v. Vasic* (n. 40).
[136] See *R. v. Cuttell, R. v. Kwok* (n. 41).
[137] *R. v. Gomboc* (n. 21), Justices McLachlin C.J. and Fish J. paras. 139-142.
[138] PIPEDA, s. 7(3).
[139] See *R. v. Cuttell* (n. 41), paras. 40 and 45.

assumption that subscriber name and address can *never* attract a reasonable expectation of privacy. As long as any subscribers have reason to expect that their name and address will not be disclosed to police by their TSP in the absence of a court order or warrant, the only general rule that will pass *Charter* scrutiny is one that respects that privacy interest.

Section 487.014 of the *Criminal Code* has also been treated as relevant to the analysis of whether subscribers have a reasonable expectation of privacy in their name and address. It states as follows:

> 487.014(1) For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing.

In *R. v. McNeice*, a B.C. court found that:

> absent a finding of state agency, s.487.014(1)provides the police with lawful authority to make a PIPEDA request for subscriber information, which an ISP is not prohibited by law from disclosing if it falls within the provisions of s. 7(3)(c.1)(ii) of PIPEDA.[140]

The Court seemed oblivious to the circularity of its reasoning. Regardless of whether the TSP is acting as an agent of the state in responding to warrantless police requests for subscriber information, this clause cannot serve as "lawful authority" under s.7(3)(c.1) of PIPEDA while at the same time relying on s.7(3)(c.1) to permit the disclosure. Section 487.014 does not therefore affect the analysis of a reasonable expectation of privacy in subscriber data.

In summary, the circumstances of the information collection being proposed – private information collected from private entities, not abandoned, subject to unknown terms of confidentiality as between the subscriber and the TSP, and not subject to any other statutory regimes that negate a reasonable expectation of privacy in the data - support a finding of reasonable expectation of privacy. Combining these circumstances with the strong privacy interest in subscriber data as a result of its function as a key to unlocking biographical core information, it is difficult to conclude that warrantless access to subscriber data would not be considered a "search" under s.8 of the *Charter*. Prior authorization is thus required.

The mere fact that key circumstances such as the subscriber agreement – or the information to which the subscriber data links, if this is treated as a circumstance – will vary by case, renders a "one size fits all" approach to accessing subscriber data inappropriate (unless such approach requires prior authorization). Putting it differently, as long as there are some cases in which a reasonable expectation of privacy inheres in the subscriber data, a general approach that makes prior authorization unnecessary will violate s.8.

[140] See *R. v. McNeice* (n. 40), para. 43.

Section 1 Analysis

Legislation that violates s.8 may still be saved if it constitutes "a reasonable limit prescribed by law as can be demonstrably justified in a free and democratic society". As noted above, the application of this test involves several steps.

Important Objective

The objective which the measures in question are designed to serve must relate to "concerns which are pressing and substantial in a free and democratic society" before it can be characterized as sufficiently important.[141] The more severe the deleterious effects of a measure, the more important the objective must be.

The objective of allowing warrantless access to subscriber data is to facilitate state investigation of crime involving telecommunications. Insofar as the effective investigation of crime is a pressing societal concern, the proposed law would seem to pass the first stage of the test under s.1. However, the Supreme Court has noted that "it is desirable to state the purpose of the limiting provision as precisely and specifically as possible so as to provide a clear framework for evaluating its importance, and the precision with which the means have been crafted to fulfil that objective.[142] The more narrow purpose of the proposal was explained by Public Safety Canada explained in a Backgrounder accompanying the introduction of Bill C-52 in November 2010:

> "Basic subscriber information is often crucial in the early stages of an investigation. Without these identifiers, the police, CSIS and the Competition Bureau often reach a dead-end, as they are unable to get sufficient information to pursue an investigative lead or obtain a warrant...the practices of releasing this information vary across the country: some service providers release the information immediately upon request; others provide it at their convenience, often following considerable delays; others insist that authorities first obtain a warrant. This lack of consistency and clarity can delay or block investigations."[143]

But aside from mere assertions about frustrated investigations, Public Safety Canada has failed to demonstrate a pressing need for this new power. As long as they have reasonable grounds, police can obtain a production order to obtain subscriber information. It is not clear how the duty to obtain such an order could "block" an otherwise reasonable and justified investigation.

---

[141] *R. v. Oakes* (n. 73), para. 69.
[142] *Thomson Newspapers Co. v. Canada (Attorney General)*, 1998 CanLII 829 (SCC) para. 98 quoted in *Harper v. Canada (Attorney General)*, 2004 SCC 33 (CanLII) para. 92.
[143] Public Safety Canada, "Backgrounder - Investigating and Preventing Criminal Electronic Communications Act" (November 1, 2011). Online: <http://www.publicsafety.gc.ca/media/nr/2010/nr20101101-1-eng.aspx last>.

Moreover, police already have at their disposal powers to forgo prior authorization where exigent circumstances exist.[144] The proposed law is therefore needed not to deal with cases of urgency or impracticality of obtaining a production order. Rather, it is designed simply to relieve the police of the burden of having to obtain a production order for this kind of data. While this would no doubt facilitate police investigations, speeding up the investigatory process is surely not "a pressing and substantial concern".

Proportionality

The proposal satisfies the first requirement of the proportionality test, that it be rationally connected to this objective: it is clearly designed to facilitate law enforcement agency investigations. However, it runs into serious problems with the next requirement of the proportionality test: minimal impairment.

Not only would law enforcement agents be empowered to force TSPs to hand over subscriber data without prior authorization, there would be no requirement for reasonable grounds to suspect, let alone believe, that an offence has been or will be committed and that the subscriber data sought will assist in the investigation of that crime. All that is required is that requests be made in the performance of "a duty or function" of the law enforcement agency.[145] This approach is in stark contrast to current provisions for warrantless searches on the grounds of exigency: in such cases the conditions for obtaining a warrant must nevertheless exist.[146] If access to subscriber data is considered to be a "search" under s.8, the proposal will fail s.1 on this basis alone.

But there are numerous other ways in which the proposal fails the "minimal impairment" test:

- in contrast to other search powers, it could be employed in the enforcement of foreign laws, even where the same laws do not exist in Canada;[147]
- there is no limit to the number of requests that can be made simultaneously or repeatedly;
- the power is not limited to crimes let alone serious offences – it would be available for use in investigating the most minor infractions under the *Criminal Code, Competition Act* and *CSIS Act*, and the collection of information for intelligence purposes would presumably be unlimited;

[144] S. 487.11, *Criminal Code*.
[145] Bill C-52, s. 16(2).
[146] S.487.11, *Criminal Code*.
[147] Bill C-52 s. 16(2)(b). There is no requirement for dual criminality in order for Canadian police services to use this provision in the investigation of foreign offences. Moreover, there is no requirement (as there is under the proposal for Preservation Orders) that authorities in the foreign state be conducting an investigation of the offence.

- there is no provision for the recipient of a demand to challenge it (in contrast to the process for challenging production orders in the proposed s.487.0193 of the *Criminal Code*);
- there is no provision for the subject to be informed of requests involving them (as is the case for interceptions);
- indeed, requests may be made subject to "gag orders" via regulation, such that subjects can never be made aware of the search involving their information;
- there is no requirement for annual public reporting on use of the power;
- there is no requirement for external audits or reviews of LEAs' use of the power; and
- there is no provision for Parliamentary review of the legislation.

In the US, designated government officials can obtain similar subscriber data[148] by way of administrative subpoena without prior judicial authorization or a showing of "probable cause".[149] However, US courts have imposed requirements regarding scope, necessity and authority to issue such subpoenas. Moreover, these subpoenas are available only for certain types of criminal investigations, notably health care fraud, child abuse, Secret Service protection, controlled substance cases, and Inspector General investigations.[150] In addition, the recipient of an administrative subpoena can challenge its validity in court on grounds that it was not issued in good faith or that its issuance or enforcement is otherwise unreasonable.[151]

None of these requirements or limitations is present in the Canadian proposal to permit law enforcement access to subscriber data without prior authorization. Other than requiring that the purpose of the request falls within the broad functions or duties of the agency, and limiting the number of agents that can make requests in the ordinary course of investigations, there are no proposed limits regarding necessity of the request or regarding the types of investigations for which such requests can be made. Nor are TSPs provided with any means to challenge individual requests.

---

[148] In addition to subscriber name, address, telephone number and IP address, "subscriber data" available to law enforcement agencies by way of subpoena includes date, time and length of communication; length of service, types of service utilized, means and source of payment for services: 18 USC 2703(c)(2).

[149] The FBI is also empowered to obtain telecommunications subscriber name, address, length of service and long distance toll billing records upon request without the need for probable cause or prior judicial authorization, for only for the purpose of foreign intelligence investigations: 18 USC 2709.

[150] US Department of Justice Office of Legal Policy, *Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities*, undated, online: <http://www.justice.gov/archive/olp/rpt_to_congress.htm#appd_b>; see also Charles Doyle, *Administrative Subpoenas and National Security Letters in Criminal and Intelligence Investigations: A Sketch,* CRS Report for Congress, April 15, 2005.

[151] DOJ Report, *id.* at 15.

Considering the numerous ways in which the proposal could be revised to be less privacy invasive while still providing law enforcement with readier access to this data, there can be no question that the proposal fails the s.1 test for minimal impairment.

Proportionality of means and ends

The final aspect of the proportionality test involves determining whether the effects of the measure so severely impinge upon individual rights that the legislative objective, albeit important, is nevertheless outweighed by the abridgement of rights. It is not necessary to go through this balancing exercise if the measure has already failed the "important objective" or "minimal impairment" test. But assuming that the proposal to allow warrantless access to subscriber data somehow passes these tests, it will undoubtedly fail on the final proportionality test.
The potentially grave intrusions on individual privacy that this proposal would permit cannot be justified by the objective of expediency in police investigations.

As explained above, names and addresses are useful to police not for their intrinsic value but rather because they allow police to attach an identity to a potentially vast, highly private and potentially incriminating collection of information about a person that has already been amassed and that can then continue to be amassed. Anonymous communications need to be protected in free and democratic societies. As noted by the Electronic Frontier Foundation,

> Many people don't want the things they say online to be connected with their offline identities. They may be concerned about political or economic retribution, harassment, or even threats to their lives. Whistleblowers report news that companies and governments would prefer to suppress; human rights workers struggle against repressive governments; parents try to create a safe way for children to explore; victims of domestic violence attempt to rebuild their lives where abusers cannot follow.[152]

The societal value of anonymous communications was recognized by the American Supreme Court in a much-cited 1995 ruling, when it stated that:

> Allowing dissenters to shield their identities frees them to express critical, minority views ... Anonymity is a shield from the tyranny of the majority... It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation ... at the hand of an intolerant society.[153]

Allowing police to pierce the anonymity of individual speech online, without any justification or prior authorization, strikes at the heart of free speech and is antithetical to democracy.

---

[152] See online: <http://www.eff.org/issues/anonymity>.
[153] *McIntyre v. Ohio Elections Commission* No.93-986, Supreme Court of the United States 514 U.S. 334 (1995) para. 357.

The damage to anonymous free speech and privacy that it would cause is not outweighed by a desire to relieve police of the need to obtain a warrant for access to subscriber data.

Applying a general rule to certain types of personal data in which individuals have a wide variance of privacy interest is dangerous, for as long as anyone has a legitimately high private interest in that data, prior authorization will be required. Thus, the only acceptable general rule will be one that respects the highest possible privacy interest in that type of data.

In brief, once it is found that access to subscriber data constitutes a "search" under s.8 of the *Charter*, it is inconceivable that a law permitting warrantless access to subscriber data could be justified as a reasonable limit in a free and democratic society.

Preservation Orders and Demands

Preservation Orders:	***Preservation Demands:***
• 90 days	• 21 days
• Authorization required	• No authorization required
• May be repeated	• No repeats

In keeping with Articles 16 and 17 of the Council of Europe's Cybercrime Convention ("*Cybercrime Convention*"), the federal government is proposing to add a new "preservation order" and "preservation demand" to the suite of new Lawful Access powers in the *Criminal Code*.

Under the proposed preservation order,[154] any police or other law enforcement officer can apply to a judge or justice of the peace for an order to preserve computer data for up to 90 days. The application must be made on oath, in writing, using a particular form. It must establish reasonable grounds to suspect that an offence under Canadian or foreign law has been or will be committed and that the computer data requested will assist in the investigation of the offence. If the offence is under foreign law, the judge or justice must be satisfied that authorities in the foreign state are conducting an investigation of the offence. Finally, the officer must have applied, or intend to apply, for a warrant or order to obtain the data in question.

The preservation order may include any conditions that the justice or judge considers appropriate, including a prohibition on disclosure of the existence of the order for a certain time

[154] Bill C-51, *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 3rd Sess, 40th Parl, 2010 (first reading 1 November 2010) [IP21C], proposed s. 487.013.

period if the justice or judge is satisfied that there are reasonable grounds to believe that disclosure during that period would jeopardize the conduct of the investigation.[155]

The preservation order would expire after 90 days if not revoked earlier. Upon revocation, expiration or production of the requested data, the person to whom the demand or order was made would be required to destroy the computer data that would not be retained in the ordinary course of business as well as any document prepared for the purpose of preserving the data.[156]

In addition to preservation orders granted by a justice or judge, police officers (and other law enforcement officers) could make preservation demands without the need for prior judicial authorization. Such demands could be made only where the officer has reasonable grounds to suspect that an offence under Canadian or foreign law has been or will be committed and that the computer data requested will assist in the investigation of the offence.[157] If foreign law, the officer must have reasonable grounds to believe that the foreign state is investigating the offence.[158] Like preservation orders, these demands could include any conditions that the officer considers appropriate, including a prohibition on disclosure of the existence or contents of the demand.[159] Preservation demands, however, would expire after 21 days and could not be repeated.[160]

Charter Analysis

Do Preservation Demands/Orders constitute "searches" or "seizures"?

The first question in a *Charter* analysis of preservation orders and demands is whether s.8 would even apply, given that the police will never come into possession of the information as a result solely of these orders and demands.

As noted above, police cannot avoid the application of the *Charter* by doing indirectly what they cannot do directly. Where they employ private actors to obtain evidence, the *Charter* will extend to the acts of those parties in their roles as "agents of the state". Applying the *Broyles* test of whether the exchange between the accused and the informer would have taken place but for the intervention of the state or its agents, it is clear that TSPs would be acting as agents of the state when they respond to preservation orders and demands (as opposed to when they provide such information to the police entirely on their own initiative). As the Supreme Court stated in *R. v. Dersch,* "[a] doctor who takes a blood sample illegally at the request of police is acting as an

[155] Bill C-51, proposed s. 487.0191 – this applies to preservation demands and production orders as well.
[156] Bill C-51, proposed s. 487.0194.
[157] Bill C.51, proposed s. 487.012(2).
[158] *Id*.
[159] *Id*. sub-section (5).
[160] *Id*. sub-section (4).

agent of government and his or her actions are subject to the *Charter*".[161] The TSP's retention of information under a preservation order/demand is thus subject to the *Charter*.

Reasonable Expectation of Privacy

In contrast to other Lawful Access proposals, preservation demands and orders are not limited to certain types of data; instead they would apply to "computer data", which is defined broadly as "representations, including signs, signals or symbols that are in a form suitable for processing in a computer system."[162] As some commentators have pointed out:

> The consequences of [preservation orders] are staggering and form the basis for our assertion that the [Council of Europe Cybercrime] convention fundamentally shifts the role of ISP from that of a conduit to a reservoir of information. For a period of up to three months, every piece of information a user inputs into the Internet, through email or Web use, could be preserved by the ISP for access by law enforcement.[163]

There can be little dispute that individuals have a reasonable expectation of privacy in the data that could be subject to these orders and demands.

Circumstances of Seizures under Preservation Orders

The same analysis applies here as applies to the proposal for warrantless access to subscriber data. The data in question is indisputably private information in the possession of private entities that value it as such. It is not abandoned by the individuals to whom it relates. It is subject to unknown terms of confidentiality as between the subscriber and the TSP. Finally, it is not subject to any other statutory regimes that would negate a reasonable expectation of privacy in the data. However, there is a critical difference: police do not actually obtain the data under preservation orders and demands. Instead, the TSP must simply preserve it, for a limited time, so as to ensure that the police are able to access the data should they obtain authority to do so within the period of the order or demand.

It is possible that this distinguishing feature of preservation orders and demands is found to substantiate a finding that they do not constitute "searches" or "seizures" under s.8, in which case the analysis ends here.

---

[161] See *R. v. Dersch* (n. 69) para. 20.
[162] Bill C. 51, clause 9(4).
[163] I. Kerr and D. Gilbert, "The Role of ISPs in the Investigation of Cybercrime", chapter 20 of Tom Mendina and Johannes J. Britz, eds, *Information Ethics in the Electronic Age* (2004) at 169.

If, on the other hand, preservation order and demands are found to constitute "seizures" under s.8 of the *Charter*, the analysis shifts to s.1. Preservation demands become presumptively unconstitutional because they do not require prior authorization and because their use is not limited to exigent circumstances. As noted by one commentator:

> Without any judicial oversight, the public must hope that the officers issuing preservation demands are able to evaluate objectively the reasonableness of their own grounds to believe that the communications they seek to preserve will afford evidence of an offence.[164]

Preservation orders, on the other hand, do require prior authorization. But such authorization is to be provided on the relatively low standard of "suspicion" (vs. "belief") that the information in question "will assist in the investigation of the offence" (vs. "afford evidence respecting commission of the offence"). As noted above, the courts have accepted this lower standard in certain circumstances even without statutory authority. Where authorized by statute, the test becomes whether the lower standard can be reasonably and demonstrably justified in a free and democratic society.[165]

Section 1 Analysis

Important Objective

The purpose of preservation orders and demands is to ensure that information potentially relevant to a criminal investigation is not lost or destroyed during a period in which police are gathering the evidence necessary to justify a production order. Given that cybercrime is a serious global problem as recognized by the Council of Europe Convention, together with the variation in TSP practices with respect to data retention, this objective is likely to pass the first part of the s.1 test.

Proportionality

The measures are carefully designed to achieve their objective. However, there is reason to question whether they do so in a minimally intrusive manner. The only safeguards against police abuse of these new powers would be:

(a) in the case of preservation orders, prior authorization on a suspicion-based standard and a 90 day limit; and

[164] Erin Morgan, "Surveillance and Privacy in the 21st Century: the Impact of Bills C-51 (IP21C) and C-52 (IPCEC)", (2011) *43 U.B.C. L. Rev*. 471-495, para. 39.
[165] *R. v. Oakes* (n. 73), para. 69.

(b) in the case of preservation demands, reasonable grounds to suspect, a 21 day limit and no repeats.

As noted above, these new powers are not limited to traffic data or other non-content data. Nor are they limited to serious offences. Indeed, they are not even limited to offences under Canadian law – further to the international *Cybercrime Convention* that Canada wishes to ratify, these powers could be used to assist foreign states in gathering evidence for the purpose of prosecutions under their laws. Yet there is no requirement for dual criminality (i.e., that the foreign offences under investigation also constitute offences under Canadian law). Nor is there any requirement that only those foreign states that have signed or ratified the Convention (which includes important safeguards in Articles 14 and 15) can take advantage of these powers. Thus, it is conceivable, for example, that the communications of a Chinese human rights activist are subject to preservation under these provisions for ultimate use by the Chinese government to prosecute that individual for what would in Canada be considered commendable free speech. The use of preservation orders for enforcement of foreign laws that are contrary to Canadian values would surely fail the proportionality test.

But there are other ways in which these new powers may be found to be unconstitutional. For example, they may be found to impair individual rights more than necessary as a result of the lack of a process for recipients to challenge a given order or demand. Although such a process would exist for recipients of production orders, it is unavailable with respect to preservation orders and demands. This is presumably because mere preservation is seen to be less intrusive than disclosure.

But the prospect of having to respond to an unlimited number of preservation demands and orders may drive TSPs to engage in routine retention of data that they would not otherwise have retained. If the cost of simply retaining communications data as a matter of course is less than the cost of responding to specific preservation orders and demands, business imperatives will result in ongoing data retention, a much more intrusive and questionable practice than request-specific data preservation – and one which would no doubt cause public uproar if proposed in Canada.

Such data retention will be limited only by PIPEDA, which requires simply that personal information be retained only as long as necessary for the fulfilment of the purposes for which it was collected, except with the consent of the individual or as required by law.[166] TSPs will likely comply with the consent requirement by simply including in their terms of service a clause purporting to obtain subscriber consent to such data retention.

In other words, business realities may turn what were intended to be narrowly targeted, time-limited "do not destroy" orders into the very kind of broad-based data retention that they

[166] Schedule 1, Principle 5.

were meant to avoid.[167] Canada will have effectively instituted an informal data retention regime similar to that in Europe (and under consideration in the US and Australia), but without any clear limits on the type of data to be retained or the period of time over which it is to be retained. Data retention laws are highly controversial because of the way they treat everyone as a suspect and make everyone's data vulnerable to unauthorized access and use.

Finally, the low evidentiary standard ("suspect"; "will assist") applicable to both powers must e assessed in light of the privacy interests affected. As noted above, any kind of "computer data" may be subject to these powers; there is no attempt to distinguish between content and "traffic data". While this may make sense in terms of the objective and the needs of law enforcement, it puts into question the appropriateness of the lower evidentiary standard.

Consistent with the *Cybercrime Convention*, the government appears to be creating a regime of evidentiary standards that varies according to the type of data in question. The rationale underlying this approach is that individuals have a greater privacy interest in the *content* of their communications than in the non-content, transmission data accompanying it. A similar regime is found in the US.[168] Under the *Criminal Code*, the lower suspicion-based standard currently applies only with respect to non-content data (production orders for financial account data, and tracking/transmission data recorder warrants). Consistent with the existing provisions, it is now being proposed for new production orders for tracking and transmission data. In all these cases, the lower standard would apply only to *non-content* data. But in the case of preservation orders and demands, it would apply to *content* data as well.

The application of a lower standard to content data under preservation orders and demands is mitigated admittedly by the fact that police must obtain a production order under the higher standard in order to access any content data preserved as a result. This is likely to be seen as sufficient justification for a lower evidentiary standard.

In summary, preservation orders and demands are likely to run into constitutional problems with respect to the absence of safeguards regarding foreign investigations. In order to ensure *Charter* compliance, the government should add a requirement of dual criminality for the exercise of these powers in the enforcement of foreign laws. As well, there is a real danger that these seemingly narrow, targeted data preservation tools have the effect of creating a *de facto* regime of ongoing data retention by TSPs in Canada, contrary to the expressed intention of the Canadian government.

New Production Orders for Transmission/Tracking Data

[167] See Public Safety Canada, "Backgrounder" accompanying Bill C-46, a previous version of the same legislation in question here, "Backgrounder: Investigative Powers for the 21st Century (IP21C) Act" Online: <http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32388.html>.

[168] *Stored Communications Act,* 18 USCS §§ 2701.

In keeping with the *Cybercrime Convention*'s distinction between content and traffic data, the Lawful Access proposals include some new production orders for non-content data, as well as revisions to existing warrants for real-time access to the same kind of data.
In each case (with one exception), the standard for disclosure or surveillance is "reasonable grounds to *suspect* that an offence has been will be committed" and that the information obtained "will assist in the investigation of the offence".

One new production order would require disclosure of "tracking data", which is defined as "data that relates to the location of a transaction, individual or thing".[169] This would include location information derived from ATM machines, GPS devices in automobiles, and GPS-enabled cell phones, among other things.

Another new production order would be available for "transmission data", defined as:

> data that (*a*) relates to the telecommunication functions of dialling, routing, addressing or signalling; (*b*) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and (*c*) does not reveal the substance, meaning or purpose of the communication.[170]

A third production order would be available for tracing a communication back to the initial service provider. This order would allow police to obtain disclosure of transmission data "related to the purpose of identifying a device or person involved in the transmission of a communication" on an expedited basis.[171] It would not require naming the TSP from whom the data is sought – instead, it would be a sort of "To Whom It May Concern" production order that would be good for 60 days. According to Public Safety Canada, this new tool is designed to help LEAs determine the origin of a particular transmission on an expedited basis, and will be useful in both domestic and international investigations.[172]

In all three cases, applications must be made in writing on oath, and the justice or judge granting the order must be satisfied that there are reasonable grounds to suspect criminal activity and that the data to be produced will assist in the investigation of the offence. This standard is lower than that applicable to general production orders and search warrants in two respects: (1) the requirement for mere suspicion as opposed to belief, and (2) the need to prove only that the data gathered "will assist in the investigation of the offence", not that it "will afford evidence

[169] Bill C-51, proposed s. 487.011, definitions.
[170] *Id.*
[171] *Id.* s. 497.015.
[172] See Public Safety Canada "Backgrounder" (n. 167).

respecting the commission of the offence".[173] This lower standard is not without precedent: it applies currently to production orders for financial or commercial information (s.487.013).

As with preservation orders, production orders may contain conditions, including gag orders. However, unlike preservation orders, they are available only with respect to the investigation of domestic (as opposed to foreign) offences.

Tracking/Transmission Data Warrants

Sections 492.1 and 492.2 of the *Criminal Code* already provide for warrants to obtain real-time information about the location of suspects and about incoming and outgoing telephone numbers, respectively. The new law would amend these provisions in a number of significant ways. In both cases, it would expand the scope of each warrant to permit remote activation and use of the devices in question, remove the requirement for the officer's oath to be in writing, and extend the maximum period of validity of the warrant in investigations of organized crime or terrorism from the normal 60 days to one year.

With respect to s.492.1 (tracking warrants), the standard for obtaining a warrant to track the *location of transactions or things* would be reworded from suspicion that "information relevant to the commission of the offence...can be obtained through use of the tracking device" to suspicion that use of the device "will assist in the investigation of the offence".[174] This provision would apply, for example, to GPS devices installed in automobiles. A new, separate warrant for tracking devices in *things usually carried or worn by individuals* would be created with a higher evidentiary standard of belief (vs. suspicion) that the tracking information will assist in the investigation.[175] This would presumably apply to real-time tracking via GPS devices in mobile phones.

With respect to s.492.2 (transmission data warrants), the low suspect/will assist evidentiary standard would remain in place, while the scope of the warrant would expand from recording incoming and outgoing telephone numbers to recording the type, direction, date, time, duration, size, origin, destination and/or termination of any communications (the same definition of "transmission data" would apply here as to production orders).[176]

Charter Analysis

[173] See Bill C-51, s. 487.012(1)(b) and 487.014(2)(b).
[174] S. 492.1(1), *Criminal Code*, and Bill C-51, proposed s. 492.1(1).
[175] Bill C-51, proposed s. 492.1(2).
[176] *Id.* s. 492.2(6).

The question of whether or not individuals have a reasonable expectation of privacy in their tracking and transmission data, whether generated by recording devices surreptitiously installed by the police or by records ordinarily generated by their service providers, is not at issue since police will continue to be required to obtain prior authorization in order to obtain this data. However, the evidentiary standard under which such warrants and production orders are granted is very much at issue.

As noted above, the Supreme Court has opened the door to a lower, suspicion-based evidentiary standard in appropriate cases, where the privacy interest at stake is reduced. Indeed, the constitutionality of the lower suspect/will assist standard for telephone number recorder warrants in s.492.2 has been upheld by one appeal court: in *R. v. Cody*, the Quebec Court of Appeal found that the data generated by a digital number recorder (telephone number and duration that the telephone was off the hook), is not sufficiently private to require the highest evidentiary standard under s.8.[177]

However, the proposed law reforms would significantly expand the scope of information subject to the transmission data warrant, and technological advances have already significantly expanded the scope of location-related information that can be recorded by way of tracking devices. These changes heighten the privacy interest at stake and should therefore affect the judicial analysis.

Transmission Data

"Transmission data", for the purposes of both the new production order and revised warrant, is defined as:

> data that (*a*) relates to the telecommunication functions of dialling, routing, addressing or signalling; (*b*) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and (*c*) does not reveal the substance, meaning or purpose of the communication.[178]

While this data may not reveal the substance, meaning or purpose of a communication, it is a significantly broader category of information than that which can be obtained through warrants for telephone number recorders under the existing s.492.2. Telephone number recorders operate as follows:

[177] See *R. v. Cody* (n. 64) para. 25.
[178] Bill C-51, proposed ss. 487.011 and 492.2(6).

> A digital number recorder (DNR) is activated when the subscriber's telephone is taken "off the hook". Electronic impulses emitted from the monitored telephone are recorded on a computer printout tape which discloses the telephone number dialled when an outgoing call is placed. The DNR does not record whether the receiving telephone was answered nor the fact or substance of the conversation, if any, which then ensues. When an incoming call is made to the monitored telephone, the DNR records only that the monitored telephone is "off the hook" when answered and the length of time during which the monitored telephone is in that position.[179]

In contrast, "transmission data recorders" will gather essentially all of the information about a communication other than the contents: type, direction, date, time, duration, size, origin, destination and termination. Moreover, through the use of sophisticated computer programs, this information can be quickly and easily compiled and analysed over time. From such information, much can be gleaned about a person's private life: who they communicate with, when and for how long each communication occurred, and whether a given electronic communication included large photographic or video files, for instance. This information can be highly revealing of a person's habits and lifestyle.

Transmission data is especially useful in making links between individuals and enabling social network analysis.[180] With transmission data, authorities can derive information about social networks – even about the relative influence of each member in the network. Indeed, they can sometimes identify a social network before the individuals themselves have appreciated its existence.[181] According to one researcher, ThorpeGlen, a British firm, sells systems that:

> analyze vast amounts of communications data in order to discover people worth investigating. Well-connected people with many links to others are not of interest. It is the isolated groups, the pairs and small groups who only connect to a few others, that draw suspicion.[182]

As well, certain devices leak data in ways that can enhance transmission data. When mobile phones are used to visit websites, for example, significant data can be accidentally made available to authorities. According to an expert mobile phone hacker, phone numbers, SIM card numbers, unique phone IDs, and the access point that is used are sometimes included with traffic data provided to US authorities.[183] There are no algorithms in existence now that 'scrub' such information from the server logs that could be turned over to police, arming authorities

---

[179] *R. v. Fegan*, (1993) 80 C.C.C. (3d) 356 (Ont. C.A.), at 363 and 364, quoted in *R. v. Cody*, (n. 67),para. 11.
[180] W. Diffie and S. Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption,* 2nd ed., (Cambridge, Mass.: The MIT Press 2007).
[181] K. J. Strandburg, "Surveillance of Emergent Associations: Freedom of Association in a Network Society", in A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. De Capitani di Vimercati (eds.). *Digital Privacy: Theory, Technologies, and Practices* (New York: Auerbach Publications, 2008).
[182] *Landau,* (n. 103) at 137.
[183] C. Mulliner "Random tales from a mobile phone hacker" Presentation at CanSecWest 2010, Vancouver, Canada. Slides online: <http://www.mulliner.org/security/feed/random_tales_mobile_hacker.pdf>.

with more information about users than they might have expected from the warrant or production order.

Moreover, the proposed revisions to s.492.2 (warrant for transmission data recorder) would recognize the increased functionality of computer-based recording devices by expanding the scope of the activities covered by the warrant beyond mere installation, monitoring and removal of devices to *remote activation and use* of the devices.[184] In other words, police powers to monitor the communications activity of suspects would be enhanced not only by obtaining more data about those communications, but also by having much greater control over the devices themselves.

There is thus a strong argument that the expanded scope of transmission data warrants attracts a level of privacy interest sufficient to justify a higher evidentiary standard than may have been acceptable for telephone number recorders.

A similar argument can be made regarding the appropriate evidentiary standard for the proposed new production orders for transmission data, especially if preservation orders can be used to ensure that transmission data is preserved by the TSP for an indeterminate amount of time. Indeed, by combining the use of preservation and production orders for transmission data, LEAs can gather the same information that they would have gathered via a transmission data warrant, the only difference being that the TSP does their surveillance for them. Either way, the data in question is potentially far more revealing than under the existing regime and thus deserves stronger protection.

Tracking Data

"Tracking data", for the purposes of the new production order and revised warrants, is defined as "data that relates to the location of a transaction, individual or thing",[185] and "tracking device", for the purposes of the warrant, is defined as "a device, including a computer program within the meaning of subsection 342.1(2), that may be used to obtain or record tracking data or to transmit it by a means of telecommunication".[186]

While these definitions do not appreciably expand the scope of the existing warrant, they apply in a context of dramatic technological improvement in location tracking devices. As pointed out by the Electronic Frontier Foundation ("EFF") and American Civil Liberties Union in their 2009 joint Amicus Brief to the United States Court of Appeals (D.C. Circuit) in the case of *USA. v.*

[184] Bill C-51, proposed s. 492.2(2).
[185] Bill C-51, proposed s. 487.011, s. 492.1(8).
[186] *Id.*

Maynard and Jones,[187] GPS tracking devices now provide a complete technological replacement for physical human surveillance: they enable 24 hours a day "dragnet" surveillance at minimal cost, they enable police to track people in private as well as public places, and they enable simultaneous surveillance of unlimited numbers of people (GPS technology can support an unlimited number of receivers). Geo-locational data from mobile communications devices is relayed by virtue of the device being turned on; disabling 'location services' does not prevent this information from being transmitted. Moreover, like other technologies, location tracking devices are getting smaller and smaller, while at the same time more powerful, making them easier to use and less prone to discovery by the subject.

Combined with the growing networks of ATMs, cell phone towers, electronic toll roads, and other electronic *means* by which location data can be gathered, the *type* of information gathered through tracking warrants can reveal far more information than used to be the case. Through deduction and inference, it can disclose a plethora of intimate information about a person's life – travel to political meetings, places of worship, news media outlets, homes of friends and family. It can also be overlaid upon demographic, psychographic, and consumer data to develop nuanced profiles that rely on Geographic Information Systems.[188] Such data can further integrate time as a variable to identify likely profiles in geographic areas throughout the day and year.[189]

This is surely information in which individuals have a strong and reasonable expectation of privacy. As the US Court of Appeals for the District of Columbia Circuit stated in a recent ruling that surreptitious surveillance via GPS devices installed in vehicles requires a warrant based on probable cause, "[w]hen it comes to privacy ... the whole may be more revealing than the parts".[190] The Court went on to explain:

> It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.[191]

---

[187] Dated March 3, 2009 online: <https://www.eff.org/files/filenode/US_v_Jones/Jones.DCCirBrief.EFFACLU.PDF>.

[188] G. Elmer, *Profiling Machines: Mapping the Personal Information Economy* (Cambridge, Mass: The MIT Press 2004).

189 See: D. Phillips and M. Curry, "Privacy and the phenetic urge: Geodemographics and the changing spatiality of local practice", in D Lyon (ed) Surveillance as social sorting : privacy, risk, and digital discrimination (London ; New York : Routledge, 2003) at 137-152.

[190] *United States v. Maynard,* 615 F.3d 544.

[191] *Id.* at 560.

The US Court of Appeals for the District of Columbia found likewise in *USA v. Maynard*, noting that the sheer quantity of information creates a picture so complete that privacy is at issue, even if each movement is in the public domain:

> A person who knows all of another's travels can deduce whether he is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts.[192]

Both cases are currently under appeal.

The information available to police through production orders for tracking data is comparable to that available through direct police surveillance via tracking devices. Yet there would be no requirement for such production orders to be individualized, nor would there be any need for reasonable grounds to suspect that the information gathered will do anything more than "assist in the investigation of the offence". Thus, police will be authorized to make bulk demands for information regarding an offence, such as all records from cell phone towers in the vicinity and around the time of the incident. As Justice Quigley of the Ontario Supreme Court noted when finding that "the sheer scope and unbridled breadth of the Tower Dump warrants [obtained under s.487] demands, in my judgment, that the evidence derived from the execution of those warrants be excluded at trial under subs. 24(2) of the *Charter*",[193]

> ... it is evident that the overwhelming and pervasive use of cell phones in Canada by an enormous percentage of the population, the advancement of cellular phone technology, and the breadth of information that may be obtained about cell phones and the people who use them, may permit such information to reveal personal and biographical matters about the users. Technological tools such as the ability to isolate and determine the cell phone traffic that passed through any particular cellular transmission tower, or simply the production of billings records with the increased information they may now capture and display, has the potential to reveal information that individuals might have expected would remain private and confidential.[194]

By continuing to apply a lower evidentiary standard to this information, the government is signalling that, while this information attracts a reasonable expectation of privacy, such expectation is not sufficiently great as to justify the normal, belief-based standard. This is disputable given the breadth and quality of information now accessible through computer-based tracking devices.

---

[192] *Id*. at 562.
[193] *R. v. Mahmood*, 2008 CanLII 51774 (ON SC), para. 48.
[194] *Id*. para. 57.

Section 1 Analysis

Assuming that the lower suspicion-based standard is found to be inappropriate for production orders for tracking and/or transmission data, or for warrants for tracking devices and/or transmission data recorders, the court will have to engage in a section 1 analysis.

The objective of the lower standards is to allow police to access more personal information with less evidence to justify their suspicions. By replacing belief with suspicion, the test allows police to proceed on the basis of less evidence – more than a hunch, but less than belief. And by requiring that the information gathered will merely "assist in the investigation of the offence", rather than that it will "afford evidence respecting commission of the offence", the lower standard opens up a trove of information to police that would otherwise be inaccessible.

The significance of these differences should not be overlooked: they will result in far more personal information being made available to law enforcement and intelligence agencies in the course of their investigations, with a correspondingly greater intrusion on individual privacy. Indeed, it can be expected that police will use these lower standards to engage in fishing expeditions under the guise of suspicion and assistance in the investigation of offences – for that is precisely what the higher standard is meant to prevent.

In order to defend the constitutionality of its application of lower evidentiary standards to these new and existing powers, the government will need to demonstrate that the lower standard is needed in order for LEAs to be able to do their jobs effectively. Such justification has yet to be provided. All that we have been told is that these provisions are needed for police to be able to fight high-tech crime – specifically "to identify all the network nodes and jurisdictions involved in the transmission of data and trace the communications back to a suspect" – and that they will "allow law enforcement officers to trace serious computer crimes such as child pornography and hate crime."[195] Yet the proposed production orders and revised warrants are in no way limited to high-tech crimes or to serious computer crimes.

Nor do they include safeguards such as reporting requirements or notice to individual subjects after the fact. While the government is proposing to expand both annual reporting requirements under s.195 and notice requirements under s.196 to cover interceptions without warrant as well as those with, it has not seen fit to require such reporting or notification in the case of s.492.1 and s.492.2 warrants. Yet, such *ex post facto* accountability measures are all the more important when the *ex ante* protections are lowered. At a minimum, the lower evidentiary standards in these proposals should be accompanied by higher standards of accountability and oversight.

While the proposals for a lower evidentiary standard are rationally connected to the important societal goal of crime prevention, they are likely to fail the proportionality test unless the

[195] Department of Justice Canada, News Release, *"*Government of Canada introduces legislation to fight crime in today's high-tech world*"*, November 1, 2010.

government can show that the benefits in terms of improved law enforcement will outweigh the costs in terms of individual privacy. There is no question that these changes will result in more state surveillance of individuals, innocent and guilty. They will also heighten the risk of police engaging in "fishing expeditions". Whether or not the societal value of purportedly improved law enforcement is worth these costs to individual privacy is a question the Supreme Court of Canada will have to confront, eventually.

Exemption for voluntary disclosure/preservation

An often overlooked aspect of the "Lawful Access" proposals involves s.497.014 of the *Criminal Code* (s.487.0195 under the proposed law reforms). The revised clause states:

> For greater certainty, no preservation demand, preservation order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing.[196]

In other words, it simply confirms that voluntary preservation and/or disclosure of information by third parties, where not prohibited by law, does not require an order or statutory demand. The proposed revisions would merely expand the scope of the existing clause to cover preservation orders/demands as well as production orders. Such changes are not an issue.

However, the clause – even as it currently exists – raises serious constitutional concerns. It purports to negate the requirement for police to obtain prior authorization where their actions invade reasonable expectations of privacy and thus constitute "searches" under the *Charter*. It ignores the fact that the *Charter* applies to voluntary third party searches where the third party acts as an agent of the state by preserving or providing the requested information. It is thus over-broad and offends the constitution by failing to restrict its application to information in which individuals do not have a reasonable expectation of privacy. The Supreme Court considered this provision in *R. v. Gomboc* in the context of a public regulation permitting electricity suppliers to disclose customer information to police as long as such disclosure is not contrary to the express request of the customer.[197] The Court found that the combined effect of s.487.014 and the regulation (together with the customer's failure to request confidentiality) established that there was "no statutory barrier" to the supplier's "voluntary cooperation with the police".[198] The constitutional issue (reasonable expectation of privacy) was determined on the basis of the regulation and other factors, without reference to s.487.014.

[196] Bill C-51 s. 487.0195(1).
[197] See *R. v. Gomboc* (n. 21).
[198] *Id*. para. 31.

Two lower court cases have taken opposite approaches to the significance of s.487.014 in the context of constitutional challenges to the voluntary collection by police of subscriber data from ISPs. In *R. v. Cuttell*, Pringle J. of the Ontario Court of Justice found that "neither the involvement of a third party nor s.487.014(1) of the *Criminal Code* can shield the police from *Charter* scrutiny if … [as here] … the ISP acts as an agent of the state in a criminal investigation".[199]

A year later, Meiklem J. of the B.C. Supreme Court disagreed that ISPs are acting as agents of the state when responding to police requests for subscriber data, and found that "absent a finding of state agency, s. 487.014(1) provides the police with lawful authority to make a PIPEDA request for subscriber information, which an ISP is not prohibited by law from disclosing…".[200] Meiklem J. seemed oblivious to the circularity of his reasoning: PIPEDA allows ISPs to disclose subscriber information to the police only if the police have identified their "lawful authority to obtain the information".[201] Needless to say, a *Criminal Code* provision permitting voluntary collection by police of information as long as the third party is not prohibited from disclosing the information cannot also serve as statutory authority for allowing third parties to make such disclosures.

To the extent that s.487.014 purports to override the constitutional requirement for prior authorization where police actions invade an individual's reasonable expectation of privacy (by engaging third parties as agents to deliver information), it cannot be given effect. For the same reason that it offends s.8 of the *Charter*, s.487.014 is unlikely to be found to constitute "a reasonable limit ...as can be demonstrably justified in a free and democratic society". If challenged under s.52(1) of the *Charter*, s.487.014 is therefore likely to be "read down" so as to apply only to situations in which the individual has no reasonable expectation of privacy in the information.

PIPEDA Reform

Closely related to s.487.014 and the proposal to mandate disclosure of subscriber data upon request is PIPEDA. Under PIPEDA, TSPs are permitted to disclose personal information (which includes name, address, and any other information about an identifiable individual) without the knowledge or consent of the individual only in certain specified circumstances. One of those circumstances is if the disclosure is "made to a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that... (ii) the disclosure is requested for the purpose of...carrying out an investigation

[199] *R. v. Cuttell* (n. 41), para. 55.
[200] See *R. v. McNeice* (n. 40), para. 43.
[201] PIPEDA s. 7(3)(c.1).

relating to the enforcement of any such law [of Canada, a province or a foreign jurisdiction]..."[202] (emphasis added).

The meaning of "lawful authority"

In the absence of clear statutory authority for police to obtain subscriber information (and other personal information) without a warrant, the term "lawful authority" has been fraught with conflicting interpretations, with some TSPs taking the position that it means a warrant or court order, and with courts struggling to determine its scope. As a result, the government has proposed to amend PIPEDA to include the following clarification:

> s.7(3.1) For greater certainty, for the purpose of paragraph (3)(*c.1*):
>
> (*a*) lawful authority refers to lawful authority other than
>
> (i) a subpoena or warrant issued, or an order made, by a court, person or body with jurisdiction to compel the production of information, or
> (ii) rules of court relating to the production of records; and
>
> (*b*) the organization that discloses the personal information is not required to verify the validity of the lawful authority identified by the government institution or the part of a government institution.[203]

While this amendment would certainly clarify that "lawful authority" does not mean a court order or warrant, it does nothing to specify what *is* required for "lawful authority" to exist. The proposed amendment therefore does little to assist courts and leaves TSPs uncertain as to when they can and cannot legally disclose customer information to the police.

One possible interpretation of "lawful authority" in the context of PIPEDA is that it simply means establishing one's credentials as a legitimate law enforcement agent acting within the scope of one's functions and duties. But this interpretation is unlikely as it is already implicit in the existing provision's requirement that the request be made by a government agent for a law enforcement purpose. As noted by Justice of the Peace Conacher in his reasons for denying a search warrant request:

> … s. 7(3) stipulates that the information can be provided without consent only if the body seeking the information has "identified its lawful authority to obtain the information" ***and*** has indicated that the disclosure is requested (in this case) for law enforcement purposes. The *Act* does not set out that the existence of a criminal investigation is, in and of itself, "lawful authority" within the meaning of the Act nor, therefore, does a "*Letter of Request for Account Information Pursuant to a Child Sexual Exploitation Investigation"* establish such

[202] *Id.*
[203] Bill C-12, *An Act to amend the Personal Information Protection and Electronic Documents Act* s. 6(12).

> authority. Accordingly, there must still be some "legal authority" to obtain the information; in the view of this Court s. 7(3)(c.1)(ii) by itself does not establish what that "lawful authority" is.[204] (emphasis in original)

Another interpretation is that "lawful authority" requires statutory authority, such as the proposed new law mandating warrantless access to subscriber data. But if by "lawful authority" the legislature meant only "statutory authority", it could and would have used that term. It must be presumed that the legislature meant more than statutory authority when it used the broader term "lawful authority".

If "lawful authority" has any meaning (other than subpoena, warrant or court order), there must be circumstances involving law enforcement when it is not present. Such circumstances could include statutory authority, common law authority and, superceding both of these, constitutional authority. Indeed, the senior policy advisor and legal advisor to the government in the drafting of PIPEDA (Stephanie Perrin and Heather Black) explained in a text entitled "The Personal Information and Electronic Documents Act: An Annotated Guide", published in 2001 shortly after the Act came into force, that:

> [Section 7(3(c.1)(ii)] … is aimed at 'pre-warrant' activities in which private sector organizations cooperate with domestic law enforcement agencies who are collecting the information on a 'casual' or 'routine' basis and for which no warrant is required. Only information that is of a relatively innocuous nature will be collected by these means, since the collection of information in which the individual has a reasonable expectation of privacy would require the *Charter* protection of a warrant.[205] (emphasis added)

Effectively refuting the now common practice of police to treat s.7(3)(c.1) of PIPEDA as authority for obtaining subscriber information from TSPs without a warrant, they note that "[w]hen … [s.7(3)(c.1)] … was introduced, the government stated that the amendment did not give any new powers to law enforcement but that it merely reflects the status quo".[206]

Later, in answer to the question "If the local police wish to obtain information about a customer, what must happen?", Perrin and Black confirm the intended meaning of "Lawful Authority" in s.7(3)(c.1):

> The organization can only comply with that request if the police can identify their lawful authority to get the information, which essentially means that it is

[204] *S.C.(Re),* 2006 ONCJ 343 (CanLII), para. 9.
[205] S. Perrin et al, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto : Irwin Law, 2001) at 75.
[206] *Id*. at 74.

> information in which the individual does not have a reasonable expectation of privacy under section 8 of the *Charter*.[207] (emphasis added).

This interpretation is buttressed by subsection 5(3) of PIPEDA which states that "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances". In other words, none of the exceptions in subs.7(3) permit collection, use or disclosure that would be considered inappropriate by reasonable persons. And surreptitious gathering by police of personal information in which the individual has a reasonable expectation of privacy would surely be considered inappropriate by reasonable people.

In other words, when a police request for information is not *Charter* compliant by reason, for example, of the lack of reasonable grounds to suspect that the information requested has anything to do with criminal wrongdoing, or because the information requested attracts a reasonable expectation of privacy, the TSP is not authorized under s.7(3)(c.1) to disclose the information. This statutory prohibition on the TSP's right to disclose perfectly mirrors the police officer's absence of constitutional authority to demand the information.

But whether a given request is *Charter* compliant is not always clear even to lawyers and judges. It is patently unreasonable to expect TSPs to be able to conduct their own *Charter* analysis with respect to each request they receive from law enforcement. For this reason alone, s.7(3)(c.1) of PIPEDA needs to be amended. But the proposed amendment would not give TSPs the certainty they need, despite stating that the disclosing organization is not required to verify the validity of the lawful authority identified. It fails to state what "lawful authority" *is* – i.e., what it would look like to a TSP who is presented with a request. "Lawful authority" needs to be positively defined as something concrete that TSPs can easily assess without legal advice.

The simplest approach that would remove uncertainty for TSPs and ensure *Charter* compliance is to remove s.7(3)(c.1) entirely, thus prohibiting disclosures of customer information in response to requests from law enforcement without a subpoena, warrant or court order. This is the strongly favoured approach of those who value civil liberties.

Alternatively, the term "lawful authority" could be replaced by "statutory authority". The government could then enact legislation such as proposed in this package of reforms permitting or requiring organizations to disclose certain kinds of personal information to LEAs upon request without a subpoena, warrant or court order. TSPs and others would then have the certainty they need regarding the legality of warrantless requests, and issues of constitutionality would focus on the legislation itself.

[207] *Id*. at 165.

Failure to distinguish between different types of personal information

PIPEDA applies broadly to all forms of "personal information" while importing notions of "appropriateness", "reasonableness" and flexibility so as to allow for differential treatment of different types of information depending on the privacy interest at stake.[208] However, most of the exceptions to the general rule against disclosure without consent set out in s.7(3) do not distinguish among different types of data; they permit the disclosure of *any* personal information as long as the conditions in the exception are met. In particular, subs.7(3)(c.1) does not distinguish between content and other, non-content data – it allows organizations to disclose any and all personal information to LEAs upon request without warrant.

This "one size fits all" approach to voluntary disclosures permitted under PIPEDA is inappropriate insofar as it fails to recognize the generally very different privacy interests inherent in different types of data. Yet, as discussed above, such differences are the basis for application under the *Criminal Code,* common law and *Charter* of different standards for permitting law enforcement access to different kinds of personal information. US law applicable to private organizations also applies different disclosure rules depending on the type of data in question, with much more stringent limits applicable to e-mail messages and other communications content than to non-content records such as subscriber name and address and session logs.[209]

Without detracting from the point that subscriber information and other non-content records can reveal a great deal about individuals and thus deserve to be protected by appropriate standards (for compelled as well as voluntary disclosure), the voluntary disclosure of personal information under s.7(3)(c.1) of PIPEDA in response to requests from LEAs, if maintained, should at least be limited to non-content information. Because they are responding to requests from law enforcement, private organizations are acting as agents of the state when providing this information. It has been clearly established that the *Charter* requires prior judicial authorization for the non-consensual interception of communications unless exigent circumstances exist, and this general rule logically extends to the surreptitious collection of data revealing the content of private communications. The exceptions set out in s.7(3) of PIPEDA that allow voluntary disclosure of personal information to police without the knowledge or consent of the individual should therefore be limited to non-content information in a manner consistent with the *Charter.*

[208] See for example s. 5(3) and Schedule 1, Principles 4.3, 4.3.4, 4.3.5 and 4.3.6.
[209] *Stored Communications Act,* 18 USC. 2702.

VII. General Comments

If, despite the analysis above, the government's proposed enhancements to Lawful Access powers are found to be constitutionally permissible, it does not follow that they are therefore appropriate or desirable. Similar powers have been in place in the US and UK for some years. The experience in those countries with expanded state surveillance powers, briefly summarized below, is instructive. It strongly suggests that Canada should think twice before adopting measures that unnecessarily expand state surveillance at the cost of individual privacy and social well-being.

Our knowledge of the effects of expanded state surveillance in the US and UK is attributable largely to regimes of oversight and accountability. Yet no similar oversight regime or accountability measures are being proposed along with the Canadian Lawful Access reform package. Deficiencies in this regard are discussed below.

Finally, it is important to put the proposed measures in the context not only of increasingly powerful tools and technologies at the disposal of law enforcement, but also of a gradual legislative and jurisprudential creep backward toward pre-*Charter* powers of state surveillance. These proposals are just one incremental move in a broader, more general tendency of Canadian governments to expand powers of state surveillance and of the Supreme Court of Canada to accept such expansion as justified in a free and democratic society.

Experience in other jurisdictions

Canada is not the only country to consider expanding police surveillance powers and capabilities in order to address the challenges of cybercrime. As noted above, the Council of Europe's *Convention on Cybercrime*, binding on those states that have ratified it, calls for signatory states to adopt legislative measures aimed at the protection of society against cybercrime and to cooperate internationally in such law enforcement.[210] What the Convention calls for include production orders and preservation orders, as well as measures to ensure that authorities can engage in the real-time collection of traffic data and the interception of communications. Most European states have ratified the Convention as has the US as a non-member state. Canada has signed but not yet ratified – the "Lawful Access" proposals under consideration now are designed, in part, to allow Canada to ratify this international treaty.

[210] See *Convention on Cybercrime* (n. 109).

The US, UK and Australia have already mandated intercept capability by telecommunications service providers operating in their territories,[211] have production orders and provided for various ways in which authorities can obtain subscriber (and other) data without prior judicial authorization or reasonable grounds.[212] The US and UK have already provided for production orders, preservation orders and warrants for traffic data in keeping with the *Cybercrime Convention* and in June 2011 the Australian government proposed legislation to facilitate Australia's accession to the *Cybercrime Convention*.[213] The availability of these new Lawful Access powers, together with the new tools that technology offers even without new powers, have led to a marked increase in state surveillance in those countries.

United States of America

As noted above, LEAs everywhere are experiencing unprecedented new surveillance capabilities as a result of new technologies. According to the US-based Centre for Democracy and Technology,

> …taken as a whole, the digital revolution has made more information available to the FBI than ever before and government surveillance goes up almost every year. In 2009, the most recent year for which statistics are available, federal and state law enforcement placed a record 2,376 wiretaps. On average, 3,763 communications were intercepted in each of these wiretaps. Far from "Going Dark" as a result of advances in technology, the FBI and other law enforcement agencies are experiencing a boon in electronic surveillance.[214]

In addition to individually authorized interceptions, TSPs in the US have reported receiving large numbers of warrantless requests for data on a regular basis, even beyond those requests made for purposes of national security.[215] According to Christopher Soghoian, a Washington, DC-based Graduate Fellow at the Center for Applied Cybersecurity Research, a company executive disclosed at a conference in 2009 that:

> Sprint Nextel [had] provided law enforcement agencies with its customers' (GPS) location information over 8 million times between September 2008 and

[211] United States: *Communications Assistance for Law Enforcement Act* (CALEA), 47 USC 1001-1010; United Kingdom: *Regulation of Investigatory Powers Act* (RIPA), chapter 23, ss. 12-14; Australia: *Telecommunications Act 1997*, parts 14- 15.

[212] *Stored Communications Act*; Administrative subpoenas are available to a wide range of US authorities for use in enforcing their statutes. In addition, the FBI is empowered to gather large amounts of subscriber and other data (not content) without warrant for purposes of counter-terrorism: 18 USC 2709. In the UK, ss.21-15 of the RIPA allows law enforcement access to transmission data upon request without warrant.

[213] Cybercrime Legislation Amendment Bill 2011 online: <http://www.aph.gov.au/house/committee/jscc/cybercrime_bill/bill.pdf>.

[214] Center for Democracy and Technology "FBI Seeks New Mandates on Communications Technologies" (February 24, 2011). Online: <http://www.cdt.org/policy/fbi-seeks-new-mandates-communications-technologies>.

[215] *Id.*

> October 2009. This massive disclosure of sensitive customer information was made possible due to the roll-out by Sprint of a new, special web portal for law enforcement officers.[216]

Facebook disclosed in 2009 that it was receiving between 10-20 requests each day from law enforcement looking for data[217] and AOL noted in 2006 that it received roughly 1,000 requests per month for data.[218] Google has disclosed that between January 2010 and July 2010, it received 4,287 data requests from law enforcement with only 128 being requests to remove content.[219]

Soghoian's research has also revealed that warrantless "emergency" requests by LEAs within the Department of Justice, to ISPs, for the content of internet communications have increased dramatically in recent years.[220] As Soghoian notes, these requests are just a small aspect of government surveillance; they do not include requests made by state and local LEAs, those made by the Secret Service or other federal LEAs outside the Department of Justice, or those requesting non-content information, such as geo-location data, subscriber information (such as name and address), or IP addresses used.

Caselaw from the US provides evidence that police there are routinely tracking suspects via GPS devices installed on vehicles and via cell phone location data, without warrants.[221] That issue is now before the US Supreme Court.[222] Also at issue is the government's right to obtain cell phone location data without warrant: several bills have been put before Congress to require warrants for such surveillance.[223] The D.C. Circuit Court of Appeals recently ordered the government to disclose information from criminal prosecutions in which law enforcement agents obtained cell-site location without a warrant.[224]

In 2009, it was revealed that the US National Security Agency had routinely examined large volumes of Americans' e-mail messages without court warrants, despite the requirement for such

---

[216] Analysis and opinion by Christopher Soghoian, "8 Million Reasons for Real Surveillance Oversight" (December 1, 2009). Online: <http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html>.

[217] N. Summers, "Walking the Cyberbeat" *Newsweek*, (April 30, 2009). Online: <http://www.newsweek.com/2009/04/30/walking-the-cyberbeat.html>.

[218] S. Hansell, "Increasing, Internet's Data Trail Leads to Court" *New York Times* (February 4, 2006). Online: <http://www.nytimes.com/2006/02/04/technology/04privacy.html>.

[219] Google "Transparency Report" (2011) online: <http://www.google.com/transparencyreport/governmentrequests/>.

[220] Analysis and opinion by Christopher Soghoian, "Warrantless "emergency" surveillance of Internet communications by DOJ up 400%" (August 4, 2011). Online: <http://paranoia.dubfire.net/2011/08/warrantless-emergency-surveillance-of.html >.

[221] See for example *United States v. Pineda Moreno* 617 F.3d 1120; and *United States v. Maynard and Jones*, (n. 187).

[222] *United States v. Maynard and Jones* is under appeal as of the writing of this paper. See also M. Hoffman "Supreme Court Agrees to Hear Key Warrantless GPS Tracking Case" Deeplinks Blog (June 27, 2011). Online: <www.eff.org>.

[223] See Digital Due Process, "EPPCA Reform: why now?" Online: <www.digitaldueprocess.org>.

[224] See Electronic Frontier Foundation Blog posting "FOIA Victory Will Shed More Light on Warrantless Tracking of Cell Phones" (September 10, 2011). Online: <https://www.eff.org/deeplinks/2011/09/eff-victory-forces-government-disclosure-court>.

surveillance to be limited to foreign intelligence. The NSA's spying on innocent citizens was so pervasive that even former President Bill Clinton's personal emails were captured.[225] In 2010, it was discovered that the FBI had, contrary to policy, issued exigent letters to collect call data and transactional information about reporters and researchers working with the *New York Times* and *Washington Post*.[226] The FBI monitored other reporters on grounds that the reporters may have received leaked information about confidential government activities.[227] Even lawyers have been subject to overzealous government surveillance authorized by post-9/11 surveillance laws, having their phone calls monitored, offices secretly searched, and homes searched.[228]

As the result of a 2009 Freedom of Information Act request, the Washington D.C.-based Electronic Privacy Information Centre (EPIC) forced disclosure of documents detailing unlawful uses of National Security Letters[229] by law enforcement agents. EPIC found that "FBI agents routinely sought documents they had no authority to procure, extended intelligence gathering activities well beyond the expiration of the agency's time-bounded authority to collect information, and failed to comply with legal protections."[230]

A recent report of the Oversight and Review Division of the Office of the Inspector General (OIG) reviewed the FBI's use of "exigent letters" and other informal surveillance powers (other than National Security Letters which were the subject of a previous report calling for corrective measures) from 2003 to 2007. The OIG found that the Bureau had not kept adequate records, had misled the courts, and had violated the *Electronic Communications Privacy Act* over the course of exercising these powers.[231] The report notes that the FBI corrected errors in their processes only after the OIG found repeated misuse by the Bureau of its statutory authority to obtain telephone records. It describes, for example, a practice known as 'sneak peeks', under which telecom company employees would respond to warrantless FBI requests by searching their databases and describing what they found to the FBI agent. Sometimes, FBI agents were even allowed to view records on the telephone company's computer screen. If the requested information was found, the FBI agents would then follow normal legal process to obtain it.[232] The report also concludes that the FBI indiscriminately requested "community of interest" or

---

[225] J. Risen and E. Lichtblau, "E-Mail Surveillance Renews Concerns in Congress" *The New York Times* (June 16, 2009). Online: <http://www.nytimes.com/2009/06/17/us/17nsa.html>.

[226] US Department of Justice, Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records" *Department of Justice* (January 2010). Online: <http://www.justice.gov/oig/special/s1001r.pdf> at 92-95.

[227] *Id*. at 115-120.

[228] E. Lichtblau "US Will Pay $2 Million to Lawyer Wrongly Jailed", *The New York Times* (November 30, 2006). Online: <http://www.nytimes.com/2006/11/30/us/30settle.html?_r=2&oref=slogin&pagewanted=print >.

[229] National Security Letters are an extraordinary search power under which the FBI can compel banks, telecommunications service providers and others to disclose customer records (but not content of communications) without prior judicial authorization or probable grounds – the FBI need only state that the information is required for counter-terrorism or foreign intelligence purposes.

[230] See Electronic Privacy Information Center, "Intelligence Oversight Board: FOIA Documents Detailing Legal Violations". Online: <http://epic.org/foia/iob/default.html>.

[231] US Department of Justice Office of the Inspector General report (n. 226).

[232] *Id.* at 47.

"calling circle" analyses of telephone numbers, likely resulting in the collection of thousands of telephone numbers that were not in fact relevant to the international terrorism investigation for which they were ostensibly collected.[233]

In a more recent report released in January 2011, the EFF concluded that "the actual number of possible violations that may have occurred in the nine years since 9/11 could approach 40,000 violations of law, Executive Order, or other regulations governing intelligence investigations."[234] EFF notes that from 2001 to 2008, the FBI itself investigated, at minimum, 7000 potential violations of laws, Executive Orders, or other regulations governing intelligence investigations. During the same period, the FBI reported to the Intelligence Oversight Board approximately 800 violations of laws, Executive Orders, or other regulations governing intelligence investigations.[235]

Post 9/11 "surveillance dragnets" in the US have also taken full advantage of information now publicly available via new technologies. The now infamous "Total Information Awareness" program was designed to gather and analyze information about individuals from all possible sources, using computer algorithms to identify patterns of behaviour, with a view to identifying terrorist suspects.[236] 'Fusion centers'[237] now regularly combine sensitive government data with publicly assessable data sets to derive inferences and actionable intelligence.[238] The Department of Homeland Security is known to have collected data from social networking sites in developing threat assessments for President Obama's inauguration.[239]

Such aggressive state surveillance has affected the perceptions of minority communities in the United States.[240] In one documented case of bureaucratic error, the leaders of an Islamic Charity were targeted by federal surveillance without warrant.[241] As noted by an FBI agent in 2009,

---

[233] *Id.* at 78.

[234] EFF, *Patterns of Misconduct: FBI Intelligence Violations from 2001 – 2008* (January 2011). Online: <https://www.eff.org/files/EFF%20IOB%20Report_0.pdf> at 12.

[235] *Id*. at 'i' and 'ii'.

[236] See Electronic Privacy Information Center ""Terrorism" Information Awareness (TIA)" Online <http://epic.org/privacy/profiling/tia>.

[237] Fusion Centers are government-supported entities that gather information from various sources, including the federal government, state, local, tribal and territorial governments, for the purpose of identifying terrorist/criminal activities and other hazards such as natural disasters. For more on fusion centers, see Torin Monahan, "The Future of Security? Surveillance Operations at Homeland Security Fusion Centres", *Social Justice* Vol. 37, Nos. 2–3 (2010–2011) , p.84; and Electronic Privacy Information Center "Information Fusion Centers and Privacy" online: <http://epic.org/privacy/fusion/>.

[238] K. Dilanian, "Fusion centers' gather terrorism intelligence – and much more," *Los Angeles Times* (November 15, 2010) Online: <http://articles.latimes.com/print/2010/nov/15/nation/la-na-fusion-centers-20101115>; see also R. Singel, "Newly Declassified Files Detail Massive FBI Data-Mining Project", *Wired* (September 23, 2009) online: <http://www.wired.com/threatlevel/2009/09/fbi-nsac/>.

[239] Tech Talk, "Homeland Security Harvested Social Network Data" *CBS News*. (October 14, 2010) Online: < http://www.cbsnews.com/8301-501465_162-20019629-501465.html>.

[240] See Landau (n. 103) at 207.

[241] EFF, "Al Haramain v. Bush", *EFF Cases* online: <https://www.eff.org/cases/al-haramain>.

"surveillance has prompted some Muslims to avoid mosques and cut charitable contributions out of fear of being questioned" or called "extremists"".[242] Needless to say, this kind of surveillance creates a climate of fear and intimidation that has a chilling effect on free speech.

United Kingdom

Electronic surveillance powers in the UK are set out in the *Regulation of Investigatory Powers Act* ("RIPA"),[243] passed in 2000, as well as the post 9/11 *Anti-Terrorism, Crime and Security Act 2001*("ATCSA").[244] Like the mandatory intercept capability proposed in Canada, RIPA requires TSPs to be capable of facilitating interception of communications and automated collection of data by LEAs. It also sets out rules under which public bodies (extending beyond LEAs to local councils) may conduct surveillance and access a person's electronic communications. Aimed at protecting the UK from terrorist attacks, the ATCSA expanded police powers in various ways, including by authorizing the disclosure of confidential information by public authorities to the police. It also established a voluntary regime of data retention by telecommunications service providers, later made mandatory further to the EU Data Retention Directive.[245]

As in the US, there has been much public opposition in the UK to the expansion of state surveillance powers in recent years, with Britain being characterized by some experts as a "surveillance society".[246] In January 2011, the Home Secretary released her findings and recommendations from an internal review of counter-terrorism and security powers, finding that "in some areas our counter-terrorism and security powers *are neither proportionate nor necessary*".[247] Noting that "communications data" (subscriber ID/address and traffic data) may be acquired by various public authorities under many legislative regimes, including the *Social Security Fraud Act* and the *Financial Services and Markets Act*, she recommended that law enforcement access to such data should be confined to that permitted under RIPA, which contains various safeguards including an oversight regime and a complaints mechanism.[248]

The Home Secretary's report follows several years of improper use of interception powers documented by the UK Interception Commissioner, including a 45% increase in monitoring

[242] As quoted in Stephen Lendman, "Lawless Spying in America to Obstruct First Amendment Freedoms," *Baltimore Chronicle and Sentinel* (October 7, 2010). Online: <http://baltimorechronicle.com/2010/100710Lendman.shtml>.
[243] 2000 ch. 23.
[244] 2001 ch. 24.
[245] Directive 2006/24/EC; UK Data Retention (EC Directive) Regulations 2009.
[246] Surveillance Studies Network, *A Report on the Surveillance Society,* for the Information Commissioner (September 2006).
[247] U.K. Home Office, *Review of Counter-Terrorism and Security Powers Review of Findings and Recommendations,* (January 2011) at 5.
[248] *Id*. at 28.

from 2006 to 2008.[249] In one case reported by the media, former police officers were found to be illegally operating a sophisticated criminal surveillance business.[250]

In July 2011, the UK-based organization Big Brother Watch released a report entitled **"**Police Databases: How Over 900 Staff Abused their Access*"*. The report found that between 2007 and 2010, 243 police officers and staff received criminal convictions for breaching the UK *Data Protection Act (DPA)*, 98 police officers and staff had their employment terminated for breaching the DPA, and 904 police officers and staff were subjected to internal disciplinary procedures for breaching the DPA.[251]

Earlier, in May 2010, Big Brother Watch released a report finding that over a two year period in 2008-2010, 372 local councils in England, Scotland and Wales had authorised 8,575 Directed Surveillance and Covert Human Intelligence Source authorisations under the RIPA.[252] BBW's research also found that innocent people had been placed under surveillance for minor infractions ranging from littering and dog fouling to smoking in a public place. One family was subject to 21 separate acts of surveillance over a 3 week period for the purpose of ascertaining the family's eligibility to send their children to a local school. Such abuses have led to proposals that local councils be divested of such powers, or at least that local council surveillance be authorized in advance by a magistrate.[253]

While there is no current proposal in Canada to give local or municipal authorities similar powers of surveillance, the staggering number of examples of documented abuses by law enforcement in the UK and the tendency to expand the uses of electronic surveillance beyond their original purposes ("function creep") in that country provide an important lesson in the dangers of expanding surveillance powers.

Summary of experience in the US and UK with Lawful Access powers

Canadians do not have to look far to find examples of how the kinds of new Lawful Access powers being proposed will be used by their own agents of law enforcement. It is unclear whether these powers have allowed authorities in the US and UK to apprehend more criminals than before; this has never been conclusively demonstrated. But it is clear that these powers have

[249] M. Kennedy, "Officials seek access to phone and email data 1,381 times a day", *The Guardian* (August 10, 2009). Online: <http://www.guardian.co.uk/uk/2009/aug/10/email-phone-intercept-requests-police>.
[250] V. Bone, "'Network' of police linked to private eyes", *BBC News* (October 2007) Online: <http://news.bbc.co.uk/2/hi/uk_news/7034317.stm>.
[251] See D. Hamilton, "Police Databases: Over 900 Police Staff Abuse their Access'. Online: <http://www.bigbrotherwatch.org.uk/Police_databases.pdf>.
[252] Big Brother Watch "The Grim RIPA: Cataloguing the ways in which local authorities have abused their covert surveillance powers". Online: <http://www.bigbrotherwatch.org.uk/TheGrimRIPA.pdf>.
[253] "Local Authorities Would Require Approval From Magistrates Before They Can Use RIPA Powers for Surveillance – Home Secretary", *eGovMonitor*, (January 27, 2011). Online: <http://www.egovmonitor.com/node/40488>.

been used to spy extensively on innocent citizens and to engage in fishing expeditions. Moreover, they have created information security risks that did not previously exist and their use appears to have exacerbated racial tensions and created a political chill. Such a track record is not promising.

Secrecy vs. Oversight/Accountability

We are aware of statistics on state surveillance in the US and UK, and on how new powers of Lawful Access are being used only because those countries have required that such information be reported and have tasked oversight bodies with making this information public. The purpose of such transparency measures is to deter LEAs from abusing their powers; reporting requirements serve as important accountability measures. This is particularly important with respect to the vast majority of electronic surveillance which is surreptitious and thus will never be disclosed to the subject of the surveillance.

In addition to mandatory reporting, some states have legislated consequences for abuse by state officials of such powers. Again, the importance of this is obvious in those instances where the victim is unlikely ever to know of the surveillance they have been subjected to.

In the UK, an independent oversight and complaints mechanism was established as part of RIPA. This includes an Office of Surveillance Commissioners to oversee covert surveillance (other than telephone interception) and ensure compliance with human rights law, as well as an Interception of Communications Commissioner and an Intelligence Services Commissioner, each of whom oversees compliance of LEAs with relevant laws. A new Investigatory Powers Tribunal was also established under RIPA to investigate individual complaints about any alleged conduct by or on behalf of the Intelligence Services.

In the US, the *Omnibus Crime Control and Safe Streets Act* requires annual reports to Congress on police wiretaps. These reports reveal the location, the kind of interception (phone, computer, pager, fax), the number of individuals whose communications were intercepted, the number of intercepted messages, the number of arrests and convictions that resulted from the interception, and the financial costs of the wiretap. Under the *Pen Register Act,* police are also required to report on their use of "PEN registers" and "trap and trace" devices[254] including the period of interceptions authorized by order and number, duration, and extension of orders, and the specific offence under which each order is given.[255] The *Stored Communications Act* requires an annual report from the Attorney General to the House and Senate Judiciary Committee on warrantless demands for data on grounds of exigent circumstances.

[254] "Pen registers" record the numbers that a target telephone is dialing. "Trap and trace" devices capture the telephone numbers that dial a target telephone.

[255] However, it appears that such reports have not always been published. See P. Schwartz, "Reviving Telecommunications Surveillance Law", *University of Chicago Law Review, Vol. 75,* No.1 (Winter, 2008), at 287.

US law also provides for civil penalties for government misconduct under surveillance laws: if the aggrieved person successfully establishes that a violation occurred, the Court may assess damages of $10,000 minimum.[256] In addition, internal disciplinary action must be taken by the department or agency concerned against officers or employees who have violated the law.

In contrast, no such oversight or accountability measures are being proposed to ensure that expanded Lawful Access in Canada is not abused by the authorities to whom it is entrusted.

Canadian Proposals for Oversight/Accountability

As noted above, the proposed new preservation demands, preservation orders, production orders and revised warrants may contain prohibitions on disclosure of the existence or contents of the order.[257] Law enforcement officers would also be able apply to the court for a specific order prohibiting a person from disclosing the existence or contents of a preservation demand, preservation order or production order during the period set out in the order.[258] Warrantless access to subscriber data would be subject to regulations that could include similar gag orders. In addition, judges would be empowered to issue warrants, preservation orders and/or production orders together with authorizations to intercept private communications, and when that occurs, the strict rules of non-disclosure to affected parties regarding interceptions would automatically apply in respect of the requests for related orders or warrants.[259]

In other words, all of these Lawful Access powers could be exercised under strict conditions of secrecy. Yet there is no proposal for public reporting of their use, for regular external audits, or for notification to subjects after the fact. Nor is there even a public body proposed or in place with powers to oversee the exercise of these powers by LEAs. While the Security Intelligence Review Committee has oversight powers over CSIS, no such body exists to oversee police activities in Canada. The Commission for Public Complaints Against the RCMP and other civilian review bodies have more limited mandates, focused on responding to public complaints about the conduct of police force members.

The Chairman of the Commission for Public Complaints Against the RCMP has also called publicly for greater powers of oversight over the national police service, pointing out that privacy and intelligence watchdogs have more power than does his office.[260]

---

[256] 18 USC 2712.

[257] Bill C-51, proposed s. 487.019(1) and s. 487.012(5).

[258] Bill C-51, proposed s. 487.0191 (Before granting such an order, the court must be satisfied by information on oath that there are reasonable grounds to believe that disclosure during the period would jeopardize the investigation).

[259] Bill C-50, proposed s. 184.2(4) and 187(8).

[260] A. Thomson, "RCMP oversight lacking, says complaints watchdog", *Times Colonist* (December 1, 2008*)*. Online:< http://www.ottawacitizen.com/RCMP+oversight+lacking+says+complaints+watchdog/1017845/story.html#ixzz1fS9PEZqr>. See also "RCMP force boss says force needs civilian oversight" *CTV News* (November 25,

His calls echo the 2007 recommendations of the Task Force on Governance and Cultural Change in the RCMP.[261] This lacuna in oversight continues to exist despite the recommendation of Justice Dennis O'Connor in his report on the Maher Arar affair that "an independent, arms-length review body" be established to oversee the information-sharing practices of the RCMP.[262] Clearly, there is a serious need for comprehensive oversight of policing and national security activities in Canada even without the proposed new expanded Lawful Access powers.

Under the Lawful Access proposals, public reporting would continue to be limited to interceptions under s.195 of the *Criminal Code* and would not extend to surveillance of a suspect's location or transmission data, nor to warrantless requests for subscriber data, preservation demands and orders, or production orders.

The current rules requiring notification of the subjects of interceptions would continue to apply to entirely surreptitious interceptions (but not to those with consent of one party such as a police informer), but would not extend to the similarly privacy-invasive surveillance via tracking devices and transmission recording devices.

And even if some of the surveillance permitted by these new Lawful Access powers was not made secret, the right of TSPs to challenge a demand, order or warrant directing them to provide information or access to information would be limited to production orders – it would not apply to preservation orders or demands, demands for subscriber data, or warrants for tracking or transmission data.

Other countries have seen fit to include a mandatory Parliamentary review of legislation granting increased powers of surveillance to their law enforcement authorities. The Canadian proposal includes no such review.

The absence of any proposal for effective oversight and accountability of LEAs exercising these new powers is a glaring omission in the Lawful Access package. As noted above, the failure to provide effective oversight is itself likely to render at least some of the proposals unconstitutional insofar as it impairs privacy rights more than necessary. Even without the proposed new powers, there have been repeated calls for more effective oversight of police agencies in Canada. It would be a serious failure of public policy to increase police powers without strengthening their accountability, especially in the current climate of mistrust based on highly publicized policing excesses.

2010). Online: <http://www.ctv.ca/CTVNews/TopStories/20101125/rcmp-william-elliott-civilian-board101125/>.

[261] Government of Canada, "Sweeping Changes Recommended in Report on Governance and Culture Change in the RCMP" (December 14, 2007). Online: <http://www.publicsafety.gc.ca/rcmp-grc/nr-eng.aspx>.

[262] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report on the Events Relating to Maher Arar,* "Analysis and Recommendations" (Sept.18, 2006), Recommendation 10.

Incremental Expansion of Lawful Access

It is also important to assess the proposed new Lawful Access powers not just on their own merits, but in the context of a series of legislative steps all heading in the same direction – toward a surveillance society.

Shortly following the 2001 terrorist attacks on New York and Washington, Canada enacted the *Anti-Terrorism Act* to give new surveillance powers to our national security agencies for the purpose of counter-terrorism and foreign intelligence gathering.[263] For example, that Act amended the *National Defence Act* so as to allow for warrantless interception of foreign communications.[264]At the same time, amendments to the *Criminal Code* gave LEAs new tools with which to fight organized crime.[265]Among their many other empowering provisions, these new laws together relaxed the *Criminal Code* requirements for electronic surveillance of suspected terrorist groups and organized crime by eliminating the need to show "investigative necessity", by extending the period of authorization from 60 days to one year, and by similarly extending the period after which the subject must be notified of the surveillance from 60 days to one year.

In 2004, a new production order was added to the *Criminal Code* for financial or commercial information.[266] By way of this new order, financial institutions could be required "to produce in writing the account number of a person named in the order or the name of a person whose account number is specified in the order, the status and type of the account, and the date on which it was opened or closed".[267] All of this information could of course be obtained via a general production order. The new production order was created solely to lower the threshold for demanding this particular kind of information, on the grounds that it does not attract the same privacy interest as, say, the details of one's financial account.

The new production orders now being proposed will follow this precedent, applying it to tracking and transmission data as well as financial account data, presumably using the same rationale. However, as noted above, the nature, quantity, quality and value of location and transmission data is changing with technology and is already potentially far more revealing of an individual's personal life than is the financial data subject to the existing special production order. In other words, even if it can be said that one's financial account number, type, status and date opened or closed does not attract such a reasonable expectation of privacy as to warrant a high evidentiary standard for disclosure, the same reasoning does not extend to tracking and transmission data.

[263] Bill C-36, 37th Parliament, 1st Session.
[264] *National Defence Act,* s. 273.65
[265]Bill C-24, 37th Parliament, 1st Session.
[266] S. 487.013.
[267] *Id.*

As noted above, preservation orders appear on their face to be a less intrusive and more reasonable solution to the problem of potential destruction of relevant data by TSPs than the mandatory data retention that some other countries have seen fit to introduce. However, business realities are such that the mere *prospect* of being frequently subjected to such demands and orders may lead TSPs to engage in data retention as a matter of course, as long as standardized data retention is less expensive than case-by-case data preservation. In other words, it is entirely possible that the apparently reasonable case-specific data preservation approach proposed in this package of Lawful Access reforms will result in a *de facto* data retention regime in Canada.

Mandatory intercept capability may also be just the first step toward an even more intrusive surveillance regime in which private commercial entities are required not just to make their *networks* intercept-capable, but to make the *devices* they sell to consumers capable of device-level monitoring. Device-level surveillance technology is already available and in use by some hackers and possibly by intelligence agencies to interfere with devices, to intercept communications in real time, and to access stored data.[268] Like other technologies, it is being constantly developed to become more functional. Device-level surveillance capacity may well become mandated in the next stage of "Lawful Access", after networks have been made fully intercept-capable.

It is increasingly evident that Canada is moving backwards toward its pre-*Charter* state of allowing extensive police surveillance without justification. The current proposals to expand Lawful Access are a big step in that direction, and of significant concern on their own. But they should also be seen in the context of what appears to be a gradual shift toward a surveillance state. It is entirely reasonable to wonder: what will be next?

[268] See for example a blog posting referring to a Chinese website that "offers mobile phone monitoring tools and services to customers who are given access to the site's backend to retrieve information". Online: <http://blog.trendmicro.com/mobile-phone-monitoring-service-found/>.

VIII. Conclusion

Under the guise of "modernization" and "keeping up with criminals", these proposals would take advantage of new technologies, new modes of communication and new social practices to significantly expand access by LEAs to the personal information of individuals. While referred to as "Lawful Access" powers, the lawfulness of some of these powers under the *Charter of Rights and Freedoms* is highly questionable.

Expanded powers would include:

- Access to "subscriber data" upon request without either prior judicial authorization or reasonable grounds to suspect criminal behaviour;
- New preservation orders, available on a low evidentiary standard;
- New preservation demands with no requirement for prior judicial authorization;
- New production orders for tracking and transmission data, available on a low evidentiary standard;
- Lower evidentiary standard for, and expanded scope of, tracking warrants,
- Expanded scope of warrants for telephone number recorders to encompass all forms of transmission data.

The government claims that the proposed legislation simply "provides authorities with the updated tools needed in the fact of rapidly changing technology, without diminishing the considerable legal protections currently afforded to Canadians with respect to privacy or freedom from unreasonable search and seizure."[269] However, the proposals do not in fact maintain the same level of police power (or privacy protection for citizens) in a changing informational context; rather, they expand police powers to access the already increased quantity and breadth of personal data now available as a result of new technologies.

This point cannot be emphasized enough: these expanded powers are not being proposed in a static context. The increased *legal* power that these proposals would expressly grant to LEAs will be greatly enhanced by the real world context of vastly more and richer personal data now available as a result of new technologies. In other words, the proposals effectively constitute a "double whammy" to individual privacy: they would give law enforcement more legal powers to mine the hugely expanded trove of personal information already available to police under existing powers.

[269] Public Safety Canada, News Release, "Government of Canada introduces legislation to fight crime in today's high-tech world", (November 1, 2010). Online: < http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32566.html>.

At a time when technology and social practices are providing LEAs with vastly greater amounts and richer types of data for investigations and intelligence-gathering, these reforms would provide such agencies with powerful new tools by which to tap this growing source of investigational data, and would do so on the basis of lower evidentiary standards - or in the case of subscriber data, no evidentiary standards at all. Individual privacy is already under siege as a result of new technologies and business practices; these reforms would further erode the fragile framework of privacy protection that we have constructed to control state surveillance.

Enhancing new LEA powers would be a requirement for TSPs to be fully intercept-capable i.e., to configure their networks so as to facilitate authorized interceptions by law enforcement agents. In addition to removing existing technical obstacles to interception by a single agent, this new law would mandate TSPs to permit multiple simultaneous interceptions by LEAs from multiple jurisdictions. Thus, the context in which police exercise their new expanded powers would be even more amenable to state surveillance, with the corollary security risk of unauthorized access and cyber-security attacks via the new mandated "back door" for law enforcement access to private communications.

One might expect that the proposals to expand police powers would be accompanied by an oversight regime with strong measures to ensure public accountability, at least where the normal requirement for prior judicial authorization is absent. Yet, there is no proposal for meaningful oversight of warrantless access powers and only a few weak measures (e.g., internal reporting and internal audits) designed to allow for some accountability. Unlike the regime governing covert interception of private communications by state authorities, there is no requirement to account publicly for the use of powers to gather data about subscribers and/or users of telecommunications services without warrant, even though data gathered in these ways can now reveal more about an individual than may be revealed by real-time interception of private communications.

Furthermore, all of the new demands, orders and warrants may be made subject to "gag orders" and, again unlike the regime governing covert interceptions by state authorities, individuals who are subject to state surveillance via the new and expanded search powers have no right to be notified of the fact. Subjects of state surveillance under these new powers are therefore unlikely ever to know of the activity unless they are eventually charged with an offence. And if individuals are unaware of searches involving them, they will be unable to challenge such searches.

Canada is not alone in proposing to expand state surveillance powers and capacity; indeed, the Lawful Access proposals are motivated to some degree by international peer pressure and Canada's desire to ratify the *Council of Europe's Convention on Cybercrime*. But the experience of other jurisdictions that have enacted similar laws in recent years is not promising: although the new laws have contributed to an explosion of state surveillance with

the inevitable accompanying misuse of powers, there is little evidence that they have actually improved state security.

Canada is in a privileged position having not yet adopted the approach of these other countries: rather than proceeding on the basis of rhetoric, we can learn from the experience elsewhere and carefully examine the evidence, weighing the costs and risks that expanded state surveillance will generate against its much less clear benefits in terms of increased security. Rather than inviting *Charter* challenges and public opposition, the government should re-examine these proposals in light of the already increased surveillance powers of LEAs and the absence of any real evidence that the proposed new powers are needed to ensure the security of Canadians.

Written by Philippa Lawson for the BCCLA

Christopher Parsons and Martin Twigg provided able technical and legal research assistance, respectively

The BCCLA gratefully acknowledges support from the Law Foundation

of British Columbia for funding this report

Funding provided by the Law Foundation of B.C.

Published by the B.C. Civil Liberties Association
www.bccla.org