



Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

October 31, 2011

VIA ELECTRONIC MAIL AND COURIER

The Honourable Vic Toews
Minister of Public Safety
269 Laurier Avenue West
Ottawa, Canada
K1A 0P8

The Honourable Robert Nicholson
Minister of Justice and Attorney General of Canada
284 Wellington Street
Ottawa, Ontario
K1A 0H8

Dear Ministers:

Introduction

As the Information and Privacy Commissioner of Ontario, I felt compelled to write to you today regarding the federal government's insistence on enacting a highly intrusive surveillance regime. I do so in full support of Canada's Privacy Commissioner Stoddart and the open letter she sent to Minister Toews on October 26th.

At the outset, please note that my mandate includes commenting on developments that affect the personal privacy of Ontarians, and overseeing law enforcement compliance with privacy legislation in Ontario. The proposed surveillance regime will have a substantial impact on the privacy rights of Ontarians, law enforcement functions, and the role of my office.

Media reports referring to Minister Toews' rejection of Commissioner Stoddart's concerns and quoting his defence of the regime suggest that the government will re-introduce Bills C-50, C-51, and C-52 ("the Bills") in essentially the same form in which they appeared in the last Parliament. In my view, that would be highly regrettable for the people of Ontario and Canada. I am writing this open letter to outline my specific concerns and concrete recommendations.

I have first summarized the privacy concerns identified by my office into five categories, followed by an in-depth discussion of each.

.../2



2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Télééc: 416-325-9188
TTY: 416-325-7539
www.ipc.on.ca

Summary of Privacy Concerns:

Reconsidering the Privacy Implications of Expanded Surveillance and Access

Before providing a detailed analysis of the privacy issues, my concerns may be summarized as follows:

- 1) The proposed powers must not come at the expense of the necessary privacy safeguards guaranteed under the *Canadian Charter of Rights and Freedoms*; in order to maintain the integrity of this constitutional framework, the government must acknowledge the sensitivity of traffic data, stored data, and tracking data.
- 2) Intrusive proposals require essential matching legislative safeguards; the courts, affected individuals, future Parliaments, and the public must be well informed about the scope, effectiveness, and deleterious effects of intrusive powers. If Parliament enacts expansive new surveillance powers, we urge the federal government to publicly commit to enacting the necessary oversight legislation in tandem.
- 3) Even with matching oversight, the proposed surveillance and access powers will require more stringent conditions precedent to determine the situations when surveillance or access may be appropriate and necessary.
- 4) The government must not impose a mandatory surveillance capacity regime on the public and its telecommunication service providers (TSPs) without adequate safeguards to protect the future of freedom and privacy; a comprehensive and public cost-benefit analysis should precede rather than follow the making of so many significant public policy decisions. Public Parliamentary hearings should be scheduled to ensure that civil society, as well as industry, have a full opportunity to provide substantial input on all of the Bills including Bill C-52 (the *Electronic Communications Act*). In addition, the *Electronic Communications Act* should be amended to require that all interception-related capacity requirements be approved by Parliament before they can be imposed.
- 5) The proposal for warrantless access to subscriber information is untenable and should be withdrawn; it remains our view that the *Electronic Communications Act* should be amended to require that the provisions setting out TSP obligations concerning “subscriber information” be deleted and replaced with a court supervised regime.

1) New Powers Must Not Come at the Expense of the Constitutional Framework

In a steady stream of communiqués dating back almost a decade and spanning 2002, 2005, 2007, 2009, and 2011, our office has cautioned against taking a legislative approach to new surveillance powers that undermines the judicially supervised rules and procedures which secure our shared rights to privacy, freedom and security of the person. Two of these were in joint communiqués led by the Privacy Commissioner of Canada, and signed by all the provincial and territorial privacy commissioners and ombudsmen (“privacy commissioners”).¹

Together, they accurately reflect the general nature of many of our current concerns and recommendations. (We also urge you to carefully consider the federal Privacy Commissioner’s November 2010 publication *A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century*.)

The concerns voiced by Canada’s privacy commissioners have been echoed by legal and academic experts specializing in technology, privacy and the law and, most importantly, by thousands of concerned Canadians who wish to have both effective law enforcement *and* strong privacy protections.

In this context, there can be little doubt that the most recent iteration of the government’s approach to expansive surveillance legislation has significant implications for personal privacy, state powers, and the longstanding constitutional compromise between the two, as well as for the oversight functions of courts and privacy commissioners, and the future of innovation, costs and competitiveness in the communications and technology fields.

The fact that the government appears to be committed to limiting real-time surveillance of private communications including in-transit e-mail under the “wiretapping” rules set out in Part VI of the *Criminal Code* is welcome news. We also welcome the absence of any public call for the creation of data retention rules with respect to subscribers and their day-to-day use of the new technologies. No such retention rules should be countenanced.

At the same time, we believe that critical elements of the proposed legislative regime suggest that the government misconceives how Canadians interact with new communications technologies and significantly underestimates the sensitivity of the personal information involved. The concomitant risks to privacy and other fundamental rights are significant.

¹ Copies of these five communiqués are available at:

December 20, 2002 - <http://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=114>; April 21, 2005 - <http://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=105>; October 10, 2007 - <http://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=662>; September 9-10, 2009 - http://www.priv.gc.ca/media/nr-c/2009/res_090910_e.cfm; and March 9, 2011 - http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.cfm.

Why? Because new surveillance powers leverage new and still evolving technologies. As a result, they significantly *increase* rather than merely maintain the state's surveillance capacity. Accordingly, attempts to frame the public debate in terms of maintaining capacity are misleading:

The ways in which we communicate with each other have undergone such enormous changes that it is entirely fanciful to say that there are simple equivalents in the Internet and broader digital domain to the communications surveillance techniques used for conventional voice-based telephones. There are many new types of communication available between individuals, but nearly all of these are in forms that are very easily computer-readable and therefore capable of complex analysis by computers. The range of tools available to law enforcement to track and link activity and database content is now vast and growing all the time. The debate is thus not about maintenance of capability but trying to determine a proper balance in new circumstances.²

In this context, the legal distinction traditionally drawn between the content of a private communication such as is exchanged during a telephone call or via e-mail and the associated *traffic* data is being overtaken by social, economic and technological developments. What we refer to as traffic data has evolved and it will continue to do so. Certainly, it is no longer confined to a list of phone numbers obtained by a dial recorder or rows of text on a telephone bill.

It extends digitally to link and trace the ongoing interactions of networks of users through unique identifying device numbers *vis-à-vis* their location in time, their location on and along the ground, their activity and interactivity within the Internet, and their relatedness within and across communities. The resulting digital trails are routinely retained by service providers and various third parties for weeks, months or even years. These trails paint a detailed and evolving picture that reflects on who we are.

Furthermore, there are strong indications that law enforcement's appetite for the surveillance of live telephone communications is being dwarfed by their interest in accessing the private content in the mass of digital trails created every time an individual sends a message, surfs the Internet, e-banks or simply carries a 3G enabled device.³ Computer facilitated analysis of this data can readily reveal the interwoven layers of core biographical information that animate communications data, particularly where the scrutiny extends for a significant period of time. As recognized by the United States Court of Appeals for the District of Columbia in a Fourth Amendment GPS vehicle tracking case being heard by the U.S. Supreme Court on November 8, 2011:

² London School of Economics, *Briefing on the Interception Modernisation Programme*, June 2009, p. 6.

³ See "[The Law Enforcement Surveillance Reporting Gap](#)" by Christopher Soghoian, Indiana University Bloomington - Center for Applied Cybersecurity Research, April 10, 2011.

Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynaecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, 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.⁴

Properly supervised, surveillance powers can be invaluable to law enforcement. However, it is equally true that where individuals are subject to unwarranted suspicions, evidence is poorly handled, or erroneous conclusions are hastily drawn, the consequences for innocent individuals can be devastating. Recent national security-related investigations make this all too clear (e.g., Maher Arar).

While we continue to support the vital law enforcement interest in pursuing electronic evidence and intelligence about serious wrongdoing, we also urge the government to ensure that any search, seizure, or surveillance of personal communications be subject to the most rigorous oversight. The constitutional values at stake demand such safeguards.

On the basis of all the above, we reject the Bills' implicit claim that the so-called non-content data elements associated with new communication devices and services are of significantly lesser constitutional significance. Safeguards comparable to those necessary to properly regulate the wiretapping of a rotary phone are required with respect to 21st century communications, including, but not limited to, rigorous prior judicial scrutiny.

2) Intrusive Proposals Require Essential Matching Legislative Safeguards

Read together, the legislative proposals substantially diminish the privacy rights of Canadians. They do so by enhancing the capacity of the state to conduct surveillance, as well as access private information, while *reducing the frequency and vigour of judicial scrutiny*, thus making it easier for the state to subject more individuals to surveillance and scrutiny.

Are the current processes that provide for oversight of surveillance-related powers sufficient to keep pace with the proposed expansion of state power? With the anticipated re-introduction of the Bills, Canadians are being asked to rely on oversight regimes designed decades ago to provide sufficient safeguards for the protection of our fundamental rights and freedoms today.

⁴ *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), cert. granted, *United States v. Jones*, 2011 WL 1456728 (June 27, 2011), U.S.S.C. Docket No. 10-1259.

The supervision provided by prior judicial authorization, the criminal trial process, and complaint-driven oversight under police and privacy-related statutes, while critical, are fundamentally insufficient. Let me explain.

The proposed surveillance and access regime will frequently involve complex, highly technical, and sensitive information. Moreover, where prior judicial authorization is required, the relevant surveillance and access applications are necessarily held *in camera* and *ex parte*. Where the resultant surveillance and access activities produce legal charges that lead to a criminal trial, the trials invariably have a narrow focus on the accused. National security-related investigations, which often have a much broader focus, invariably proceed in secrecy, and are rarely subject to public scrutiny. In both contexts, innocent individuals subject to surreptitious invasions of their privacy may never be in a position to learn about, let alone file for or find any redress. In addition, existing complaint regimes are limited as to their reach, powers and remedies. Any in depth public scrutiny of such matters will be the *rare* exception to a general rule of confidentiality and secrecy.

Furthermore, under the Bills, local, provincial, and federal law enforcement agencies will be equally empowered to use these intrusive powers in pursuit of both domestic and international investigations. Without a focused harmonizing and coordinating authority, inconsistent policies and practices are likely to develop among the various jurisdictions. Inevitably, privacy rights and civil liberties will suffer from fragmented and inconsistent protections.

Canadians have a *constitutional* right to be secure from unreasonable search and seizure. The expansive surveillance proposals bring this right into question. And, since the state's authority to intrude on privacy does not come with concomitant responsibilities with respect to accountability, notification and transparency, the net negative effect on human rights is likely to be compounded over time.

To its credit, the government has responded to recent court rulings⁵ by including a provision in Bill C-50 that will require that: (i) a person who has been the target of a warrantless exceptional circumstances interception must be notified of the interception within a specified period; and (ii) the relevant Minister must report publicly on police resort to such warrantless wiretaps.

At the same time, we note that these notice and reporting mechanisms are confined to providing a modest degree of notice, transparency and accountability (restricted as they are to only notifying the *target* of the surveillance, and confined as they are to limited numeric reporting) with respect to a single surveillance power – the power to intercept a private communication. In addition, the reporting practices of provincial and federal Attorneys General with respect to the use of these Part VI wiretap powers have varied considerably (as seen in jurisdictions where the required annual reports have sometimes not appeared until several years have passed).

In this context, we call for the government's public commitment to the enactment of sufficient safeguards to match the array of new and existing powers.

⁵ See *R. v. Six Accused Persons*, [2008] B.C.J. No. 293 (S.C.) and *R. v. Riley*, [2008] O.J. No. 2887 (S.C.J).

Support for this call can be found in recent U.S. and Canadian court decisions. In a unanimous decision of September 6, 2011 requiring the U.S. Department of Justice to publicly disclose information showing the government's use of cell phone location data in criminal prosecutions resulting in a guilty plea or a conviction, the United States Court of Appeals for the District of Columbia determined that:

The disclosure sought by the plaintiffs would inform ... ongoing public policy discussion by shedding light on the scope and effectiveness of cell phone tracking as a law enforcement tool. It would, for example, provide information about the kinds of crimes the government uses cell phone tracking data to investigate. As the plaintiffs note, with respect to wiretapping Congress has balanced privacy interests with law enforcement needs by permitting the government to use that technique for only the more serious offenses ... and the plaintiffs (and others) may decide to argue for similar legislation to govern cell phone tracking. Disclosure would also provide information regarding how often prosecutions against people who have been tracked are successful, thus shedding some light on the efficacy of the technique and whether pursuing it is worthwhile in light of the privacy implications.⁶

And, as indicated above, recent rulings of the Superior Courts of Ontario and British Columbia have determined that notice and reporting safeguards are constitutionally required with respect to intrusive surveillance powers, such as the power Parliament granted peace officers in section 184.4 of the *Criminal Code* (a power to conduct warrantless wiretapping in certain exceptional circumstances). For example, in *R. v. Six Accused Persons*, the B.C. Supreme Court determined that:

Although the Crown submits that in most cases where ... persons whose communications have been intercepted will receive *de facto* notification by way of the prosecution of the underlying offence, that submission fails to recognize that the communications of persons other than the alleged perpetrator may have been intercepted. It also fails to address situations where, for whatever reason, the police may have erred in their assessment of the need to intercept private communications, intercepted more communications than those to which they were lawfully entitled or over a longer period of time, or those that were intercepted under circumstances which did not result in a prosecution.

In any or all of those circumstances, the police would be answerable to no one. Further, the fact that there is no obligation to disclose surreptitious invasions of privacy to those persons whose communications have been intercepted removes an important safeguard to the potential abuse of power that can arise without accountability.

⁶ *American Civil Liberties Union v. United States*, United States Court of Appeals for the District of Columbia Circuit, September 6, 2011, No. 10-5159.

This case is illustrative of some of those concerns ... To this day, many of the persons whose communications were intercepted by the police are unlikely to know of that invasion of their privacy. That circumstance is exacerbated by the police having engaged in the automatic monitoring of all calls to the telephones they had identified as being appropriate for interception. Any discovery by third parties of the police having intercepted their private communications would be fortuitous.

Requirements to notify persons whose private communications have been intercepted of the fact of that interception afford an important constitutional and accountability safeguard to the potential abuse of state power in invading the privacy of its citizens.

The interception of private communications in exigent circumstances is not like situations of hot pursuit, entry into a dwelling place to respond to a 9-1-1 call, or searches incidental to arrest when public safety is engaged. In those circumstances, the person who has been the subject of a search will immediately be aware of both the circumstances and consequences of police action. The invasion of privacy by interception of private communications will, however, be undetectable, unknown and undiscoverable by those targeted unless the state seeks to rely on the results of its intentionally secretive activities in a subsequent prosecution.

I am accordingly satisfied that the failure of ... the [*Criminal Code*] to provide notification of surreptitious interception of private communications to those persons whose communications are intercepted is a serious impediment to the constitutional validity of s. 184.4.

.....
If the intention of Parliament in requiring the provision of [public] reports [enumerating resort to surveillance powers] is to oversee the frequency and circumstances of the interception of private communications by the police, the failure to provide a similar reporting requirement under s. 184.4 of the *Code* removes the potential for that oversight. As with the failure to require notification of those intercepted of the fact of an interception, the lack of any reporting requirement undermines both constitutionality and police accountability.⁷

Bearing all of the above in mind, and in addition to the adjustments we call for to Bills C-51 and C-52, we renew our call for the creation of an independent, arm's-length *Surveillance and Access Review Agency (SARA)*, with a legislative mandate to supervise state access to the highly sensitive personal information associated with digital communications and to report annually to Parliament and the public on the use of the surveillance and access powers.⁸

⁷ *R. v. Six Accused Persons*, [2008] B.C.J. No. 293 (S.C.)

⁸ For more information about the functions and duties we propose for *SARA*, please see our [April 21, 2005 letter to the then Minister of Justice and Attorney General of Canada](#).

In establishing *SARA*, Parliament would require law enforcement and security agencies who obtain any communication-related data from TSPs to notify all of the individuals whose personal information is involved within one year of the information being obtained unless the individual cannot readily be identified or reasonably located, or notification would prejudice an ongoing investigation. Notification of all readily identifiable individuals would be required within five years of the information being obtained unless, on application to *SARA*, it is determined that the public interest in non-disclosure outweighs the right to notification.

In this context, TSPs should be required to publish annual reports on how many interception and access orders (and requests) they receive a year from which law enforcement and security agencies, in respect of how many individuals; and how many orders (and requests) result in the disclosure of personal information, and in respect of how many individuals.

In renewing the call for the creation of *SARA*, we acknowledge that the preparation and enactment of the necessary legislative framework will take time and that, in the meantime, the government may well decide to proceed with its plan to substantially reshape the state's capacity to conduct surveillance. To the extent that you are not prepared to redraft the Bills to ensure that the new surveillance powers are justified and that the necessary safeguards are in place before the regime comes into force, we strongly urge you to publicly commit to enact a *SARA Act* in tandem with the proposed surveillance and access regime, even as you move to amend the current legislative proposals to provide additional if limited safeguards on it coming into force, as further discussed below.

3) Even with Matching Oversight, the Proposed Powers Require Adjustment

Bill C-51, the *Investigative Powers for the 21st Century Act*, will amend the *Criminal Code*, giving "peace officers" and "public officers" new avenues to obtain access to information generated electronically. As such, a wide range of officers, extending well beyond police, will be empowered to:

- Issue preservation demands on their own say so with respect to a wide array of primarily corporate-held data in the course of investigating any offence, including on behalf of a foreign state, and impose any conditions in the demand that they consider appropriate, including conditions prohibiting the disclosure of its existence or some or all of its contents,
- Apply for new suspicion-based preservation and production orders to preserve and gain access to information about transmission, traffic, communication, tracking, transaction and financial data,
- Apply for new suspicion-based warrants to enable the remote live tracking of vehicles and other things,
- Apply for belief-based warrants to enable the remote live tracking of individuals by tracking the location of cell phones or other things they usually carry or wear, and
- Apply for non-disclosure/secretcy orders with respect to all of the above.

It is our view that, as a general rule, law enforcement access to data, particularly communications-related data, as well as the new tracking powers, should be subject to prior judicial scrutiny, limited to the investigation of serious crime, generally subject to higher belief rather than suspicion-based thresholds, and come with additional oversight and accountability-related safeguards.

In this context, I note that an August 22, 2011 U.S. District Court decision invites us to raise the question as to the constitutionality of the proposed suspicion-based, as well as belief-based, production order making powers.⁹ In this case, the U.S. government had asked the Court for “orders directing Verizon Wireless, a cell-phone service provider, to disclose recorded information of cell-site-location records for one of its customers pursuant ... to the *Stored Communications Act* or ‘SCA’.” The proposed order sought stored, historical cell-site-location records tied to a period in excess of 113 days. On its face, the *SCA* provides that such an order “may be issued by ... a court of competent jurisdiction ... only if the governmental entity offers specific and articulable facts showing that there are *reasonable grounds to believe* that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” (Emphasis added.) The Court determined that “the Fourth Amendment to the United States Constitution requires a warrant and a showing of probable cause before the Government may obtain the cell-site-location records requested here.”

As the Court clearly understood, the problem with these kinds of production orders is their implication for the privacy of society at large and, in my view, the concerns expressed by the Court with respect to Americans apply equally with respect to Canadians:

The vast majority of Americans own cell phones. Many Americans have abandoned land line phones entirely, and use cell phones for all telephonic communications. Typically people carry these phones at all times: at work, in the car, during travel, and at home. For many Americans, there is no time in the day when they are more than a few feet away from their cell phones.

Cell phones work by communicating with cell-sites operated by cell-phone service providers. Each cell-site operates at a certain location and covers a certain range of distance. The number of cell-sites that must be placed within a particular area, and thus the distance between cell-sites, is determined by several factors, including population density.

If a user’s cell phone has communicated with a particular cell-site, this strongly suggests that the user has physically been within the particular cell-site’s geographical range. By technical and practical necessity, cell-phone service providers keep historical records of which cell-sites each of their users’ cell phones have communicated.

⁹ *In the matter of an application of the United States of America for an Order authorizing the release of historical cell-site information* No. 10-MC-897, United States District Court, E.D. New York (August 22, 2011).

The implication of these facts is that cellular service providers have records of the geographic location of almost every American at almost every time of day and night. And under current statutes and law enforcement practices, these records can be obtained without a search warrant and its requisite showing of probable cause.

What does this mean for ordinary Americans? That at all times, our physical movements are being monitored and recorded, and once the Government can make a showing of less-than-probable-cause, it may obtain these records of our movements, study the map our lives, and learn the many things we reveal about ourselves through our physical presence.

In the same vein, in the *Maynard* case now pending before the U.S. Supreme Court, the reasoning of the United States Court of Appeals for the District of Columbia provokes questions as to the constitutionality of the proposed suspicion-based, as well as belief-based, *tracking* warrants. As the Appeal Court found in *Maynard*, “prolonged GPS monitoring [of a person’s vehicle travelling on public roads] defeats an expectation of privacy that our society recognizes as reasonable” and must comply with Fourth Amendment standards.

The Court’s holding was echoed as recently as September 21, 2011 in a report issued by the *Liberty and Security Committee* of the U.S. *Constitution Project*. This bi-partisan committee, whose members include two former members of Congress, former FBI director William Sessions, a former U.S. Court of Appeals judge and a former chair of the American Conservative Union, concludes that “when powerful tracking technologies to conduct pervasive surveillance are paired with [a computer’s] analytic capability and a digital database, such monitoring can violate an individual’s reasonable expectation of privacy even in a public place.”

The Committee recommends that, if the U.S. Supreme Court does not adopt the proper approach in the *Maynard* case, Congress should do so by enacting legislation requiring court warrants for any location tracking lasting more than 24 hours.¹⁰

Consistent with these developments, in my view, it is essential that more stringent conditions precedent be enacted in relation to the proposed surveillance and access powers. The use of production orders and tracking warrants should be confined to investigations in respect of the list of serious offences in section 183 of the *Criminal Code*. Before issuing such orders or warrants, a superior court judge ought to be satisfied that:

- There are reasonable and probable grounds to believe that an offence under section 183 of the *Criminal Code* has been or is being committed,
- Other less intrusive investigative methods are likely to prove impracticable,

¹⁰ See the Liberty and Security Committee September 21st, 2011 *Statement on Location Tracking* at <http://www.constitutionproject.org/pdf/LocationTrackingReport.pdf>.

- Measures will be taken to safeguard the privacy of the personal information obtained, particularly of non-suspects, and
- The intrusion is otherwise in the best interests of the administration of justice.

As indicated, Bill C-51 also proposes to create a new set of powers that police could invoke to require data managers to locate and hold personal information in documents or databanks. Government has argued that these preservation powers are necessary to support the production order powers discussed above. In our view, any power to issue a preservation demand or order should be confined to the same list of serious offences in section 183 of the *Criminal Code*.

In addition, in order to address the risk to accountability that non-disclosure or secrecy orders entail, we recommend that all those whose personal information is obtained under a surveillance and access regime should be entitled to notification at the appropriate time. And, in accord with our *SARA*-related recommendations, state use of these powers and access to this personal information should be superintended and reviewed by an independent agency.

It is also noteworthy that in introducing sections 487.0195(1) and (2) to the *Criminal Code*, Bill C-51 provides broad immunity from “any criminal or civil liability” to any person who voluntarily preserves data or provides a document to an officer. The person is no longer required to show that he or she acted on reasonable grounds *per* the operation of what is now section 487.014 with section 25 of the *Criminal Code*. The person need only show that his or her cooperation was not “prohibited by law.” In our view, individuals and entities responsible for safeguarding personal information of members of the public must act reasonably before they should be entitled to such immunity. A reasonableness standard provides volunteers with significant protection while helping to rule out the possibility that, for example, malicious or incompetent decision makers will enjoy undeserved immunity.

Accordingly, section 487.0195(2) should be amended to provide that:

A person who preserves data or provides a document in the circumstances described in subsection (1) does not incur any criminal or civil liability for doing so if he or she acted reasonably in the circumstances.

Bill C-50, the *Improving Access to Investigative Tools for Serious Crimes Act*, will amend the *Criminal Code*, first by providing that if a wiretap authorization is granted under Part VI, the judge may at the same time issue one or more Bill C-51-related warrants or orders that relate to the investigation in respect of which the wiretap authorization is given. That is, in obtaining a wiretap warrant, police may also contemporaneously obtain companion production orders and tracking warrants, all from a single judge. Rules respecting secrecy and confidentiality that apply in respect of a wiretap authorization will also apply in respect of a request for a related warrant or order. In addition, the Bill will permit a peace officer or a public officer to install and make use of a number recorder without a warrant in exigent circumstances. The Bill will also extend to one year the maximum period of validity of a warrant for a tracking device and a number recorder if the warrant is issued in respect of a terrorism offence or an offence relating to a criminal organization (the maximum is now 60 days).

The critical development brought forward in Bill C-50 is that the efficiencies it may purchase in streamlining the conduct of judicially authorized state surveillance and access may come at some cost to the rigour of prior judicial scrutiny. In some cases, a single judge hearing a multitude of inter-related applications may be better informed about the extent of the overarching surveillance employed. At the same time, the demands on judges are likely to grow. In the context of what are necessarily *ex parte* and *in camera* proceedings, there will be an increased risk that a greater degree of intrusive surveillance and access will be granted in cases where it is not warranted. While we do not oppose Bill C-50 *per se*, its enactment will likely intensify the effect of the new surveillance regime. Such intensification increases the need for the adoption of matching safeguards under a *SARA Act*.

4) Surveillance Must Not Undercut the Future of Freedom, Innovation and Privacy

In addition to the controversial plan to provide law enforcement with warrantless access to subscriber information (discussed in section 5 below), the *Electronic Communications Act* sets in motion a fundamental change to the way communication services are regulated. It does so by entrenching the power of security officials to require TSPs to:

- Build in and continuously maintain a wide array of yet to be specified interception capabilities into all their networks, systems and software for the purpose of allowing authorized agencies to intercept, isolate and accurately correlate multiple communications per court orders,
- Notify law enforcement and CSIS officials regarding changes to state provided equipment or systems where those changes are likely to reduce interception capability;
- Assist designated persons who will have warrantless access to TSP facilities, systems, documents and information to test, inspect, and access TSP facilities, services and systems for regulatory purposes,
- Provide prescribed specialized telecommunications support to CSIS and law enforcement agencies,
- Submit lists of TSP personnel to CSIS and/or the RCMP for the purposes of conducting security assessments of employees who may assist in the interception of communications, and
- Comply with prescribed confidentiality and security measures.¹¹

The *Electronic Communications Act* will also establish numerous offences and violations and subject TSPs, their officers, directors, and employees to prosecution and fines for failing to comply with obligations, including those relating to systems requirements.

¹¹ Note that, to date, security officials have been able to impose a similar framework largely outside Parliamentary scrutiny through, for example, the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications, and Conditions of Licence for New Cellular and PCS Licences issued by the Minister of Industry under the *Radiocommunication Act* (see <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf09251.html>).

Each additional day in breach of the statute will add to the count of violations and increase the exposure of TSPs, their officers, directors, and employees to fines of up to \$50,000 per offence for an individual and \$250,000 for a corporation. The *Electronic Communications Act* will allow the state to seek a court injunction ordering a TSP to cease operating a transmission apparatus, or to refrain from acquiring, installing or operating new software, if the TSP is contravening or likely to contravene interception requirements.

It is also noteworthy that the *Electronic Communications Act* does not address the financial and commercial implications of these proposals, either to businesses, consumers, or taxpayers. It only authorizes the payment of some monies to compensate TSPs in relation to: (i) compliance with a Ministerial order to provide interception capabilities additional to those prescribed; (ii) the provision of subscriber information; and (iii) the provision of certain specialized telecommunications support. Reports about the cost of related proposals in the U.S. and the U.K. warrant careful consideration in Canada.

In October of 2010, it was reported that, in response to the Obama administration's intention to submit comparable surveillance legislation, American TSPs are "likely to object to increased government intervention in the design or launch of services. Such a change ... could have major repercussions for industry innovation, costs and competitiveness."¹²

In the U.K., a related though more intrusive data retention and "Interception Modernization Program" was being considered until it was abandoned by the British government in late 2009 because of concerns about cost, controversy and feasibility. Prior to this, it was reported that development costs will be high (2 to 13 billion pounds). "The bulk of the costs will be incurred by [TSPs]. The most ignored cost comes in the form of opportunity costs as engineers will be tasked to develop this [surveillance] solution instead of developing their core business, *i.e.* new ways to enhance the networks for advancing consumer and business interests."¹³

None of these immediate financial costs would necessarily translate into privacy issues *per se* if it were not for the fact that the *Electronic Communications Act* risks causing additional marketplace distortions by effectively prohibiting the use and development of any systems or software that might impair a TSP's capacity to facilitate simultaneous multiple intercepts. While the goal of facilitating compliance with court ordered surveillance is valid, there is a significant risk that in implementing this legislation, the authorities will impede the development and use of new communications technologies and services, particularly, for example, privacy enhancing technologies and services such as those that provide for encryption.

In this regard, the *Electronic Communications Act* requires that a TSP must "use the means in its control" to provide an intercepted communication "in the same form as it was before the communication was treated by the service provider" by way of encoding, compression, or encryption. A TSP is not required to make the form of an intercepted communication the same as it was before the communication was treated if it would be required to develop or acquire new

¹² "Officials Push to Bolster Law on Wiretapping", Charlie Savage, New York Times, October 18, 2010.

¹³ London School of Economics, *Briefing on the Interception Modernisation Programme*, June 2009, p. 44-45.

decryption techniques or tools. The legislation appears to allow companies like Research in Motion to continue to provide existing encryption protected communication services. It remains to be seen what the future holds for new companies and new strong encryption techniques and services in the field of communications. For example, there is a risk that the *Electronic Communications Act* will set the stage for rules requiring back-door state access to encryption services.

It is evident that many of the critical details flowing from the *Electronic Communications Act* will be left to policies, procedures, regulations and evolving relationships between TSPs and the state. In passing so many significant public policy decisions on to security-oriented officials, Parliamentarians and the public risk being left out of the decision-making process and Canadians risk seeing TSPs transformed into agents of the state. This represents a significant and needless risk to a free and open society.

We only have to look to recent U.S. history to consider the implications. Many will now be familiar with reports of the secretive and controversial assistance that major telecommunications carriers provided the National Security Agency in the conduct of warrantless eavesdropping on international calls by suspected terrorists after 9/11. As recognized by U.S. courts, such surveillance has the potential to expose “journalistic sources, witnesses, experts, foreign government officials, and victims of human rights abuses located outside the United States” to “violence and retaliation by their own governments, non-state actors, and the U.S. government.”¹⁴

While the *Electronic Communications Act* will be subject to a form of Parliamentary review five years out, in the meantime, if passed, it will substantially alter the design and operation of communication systems, the role and function of TSPs, their ability to be transparent, and the relationship between citizens, TSPs and the state.

A comprehensive and public cost benefit analysis should *precede* rather than follow the making of so many significant public policy decisions. Before imposing the kind of interception capacity regime the *Electronic Communications Act* would impose on TSPs, Parliament should ensure that such a capacity regime will be proportionate and designed to ensure not only appropriate surveillance capacity but also necessary competitiveness and privacy.

It follows that the Parliamentary committee eventually mandated to consider the kinds of proposals in the *Electronic Communications Act* should be adequately resourced to ensure that civil society, as well as industry, has a full opportunity to provide substantial input.

In addition, the *Electronic Communications Act* should be amended to require that all interception-related capacity requirements be *publicly* vetted for their impact on privacy and competitiveness *before* they are imposed (in the future, *SARA* should have a role to play in reporting on the impact of capacity-related requirements). Such requirements should be

¹⁴ *Amnesty Int'l USA et al. v. Clapper et al.*, United States Court of Appeals for the Second Circuit, September 21st, 2011, 09-4112-cv, at pages 8-9 of Circuit Judge Lynch's decision, quoting from *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011).

provided for in the form of draft regulations which would only come into force after a vote by Parliament to approve them as a whole.

5) Warrantless Access to Subscriber Information Must Be Withdrawn

In addition to providing the state with substantial control over the design and operation of TSP systems, the *Electronic Communications Act* will also provide law enforcement and CSIS officials with *warrantless* access to subscriber information for the purposes of performing *any* of their duties or functions. Subscriber information includes a named individual's IP address or mobile ID number, or the name and contact information of a subscriber associated with an IP address or mobile ID number.

The *Electronic Communications Act* provides for attenuated *post facto* review of warrantless access to subscriber information. In doing so, it relies on provincial and territorial privacy commissioners to: (i) conduct audits to assess local and provincial police compliance with provisions of the statute empowering the collection and use of subscriber information; and (ii) review police reports generated to the extent that police decide that something has occurred with respect to their own exercise of these access powers that, in their opinion, ought to be brought to the attention of the responsible provincial minister (in Ontario, the attorney general).

Under section 20(6) of the legislation, the Privacy Commissioner of Canada must provide Parliament with an annual report identifying the provincial and territorial privacy commissioners who may receive any such opinion-based reports and the powers that they have to conduct section 20 compliance audits.

Like a number of other provincial and territorial privacy commissioners, I lack the necessary powers. In particular, under Ontario's privacy statutes, I do not have any audit powers. Even those privacy commissioners with sufficient powers are likely to need additional resources in order to adequately perform the legislative duties imposed under section 20 of the *Electronic Communications Act*.

In a letter of March 9, 2011 signed by all the federal, provincial and territorial privacy commissioners, we joined our colleagues in calling on the federal government to commit to working with provincial and territorial governments to ensure that all of our offices have sufficient powers and resources should the *Electronic Communications Act* be enacted. It does not appear that any such commitment has been forthcoming.

Quite apart from the constitutional issues raised by the enactment of a regime of warrantless access, it is noteworthy that in some circumstances, aspects of *post facto* oversight of communications-related surveillance powers have been found by Superior Courts to be constitutionally required (see, for example *R. v. Six Accused Persons*, [2008] B.C.J. No. 293 and *R. v. Riley*, [2008] O.J. No. 2887). In the absence of the necessary provincial and territorial powers and resources, the *Electronic Communications Act's* reliance on provincial and territorial privacy commissioners is untenable. In addition, the audit duties to be imposed on provincial and territorial privacy commissioners under section 20 may raise division of powers problems.

It remains our view that the *Electronic Communications Act* should be amended to require that provisions setting out TSP obligations concerning “subscriber information” should be deleted and replaced with a court supervised regime.

“Subscriber information” is personal information. To date, all individual customers enjoy the legal right to insist that, subject to narrowly defined exceptions, their subscriber information remains private and confidential. The law currently provides for warrant procedures, expedited tele-warrants, and an organization’s special exercise of discretion to disclose personal information to law enforcement without an individual’s consent, for example, in aid of an Internet-related child pornography investigation, or in comparable exigent-like circumstances. Granting law enforcement and intelligence officials an almost unfettered power to issue their own administrative “warrants” for the purposes of performing *any* of their duties or functions is a substantial departure from the legal and constitutional framework in Canada. Such a departure requires extraordinary justification and a substantial framework for accountability.

Consistent with our earlier comments, law enforcement and security agency access to information linking subscribers to devices (and *vice versa*) should generally be subject to prior judicial scrutiny accompanied by the appropriate checks and balances. Before issuing an order requiring the disclosure of subscriber information, a judge ought to be satisfied that:

- There are reasonable and probable grounds to believe that an offence under section 183 of the *Criminal Code* has been or is being committed,
- Measures will be taken to safeguard the privacy of the personal information obtained, particularly of any non-suspects, and
- The intrusion is otherwise in the best interests of the administration of justice.

In the alternative, if Parliament is determined to allow warrantless access to subscriber information, the legislative safeguards in section 20 of the *Electronic Communications Act* should be strengthened so that they provide a much greater degree of *post facto* oversight. In particular:

- The power to demand warrantless access to subscriber information should be narrowed to only apply in circumstances where access is necessary to the investigation of a specific and defined category of serious crime, for example, sexual offences involving children and minors, or to prevent or eliminate a significant and imminent risk of serious bodily harm.
- The “consistent use” limitation regarding subscriber information collected by law enforcement and security agencies should be strengthened. A use should only be considered as consistent if a reasonable person might reasonably have expected such a use.

- Law enforcement and security agencies should be required to securely destroy information that is provided in response to a subscriber information request one year after the individual has been notified of its collection, or once retention of the information is no longer necessary for the purpose for which the information was obtained, or for a use consistent with that purpose, whichever is later.
- The requirement that law enforcement and security agencies must report to attorneys general and privacy commissioners should be strengthened. Agencies should be expressly required to report any collection, use or retention practices that do not appear to be necessary and proportionate in relation to the duty or function for which they were originally obtained.
- In reporting to Parliament on the adequacy of audit and investigation powers available to provincial and territorial privacy commissioners, the Privacy Commissioner should also report on whether those commissioners consider themselves to have adequate resources to conduct the necessary audits and reviews.
- If, after consulting with a provincial or territorial commissioner, the Privacy Commissioner reports that her colleague does not have substantially similar powers, the subscriber information powers available to police services within that jurisdiction should *automatically* lapse until the Privacy Commissioner reports back that the provincial or territorial commissioner has been provided with those powers.

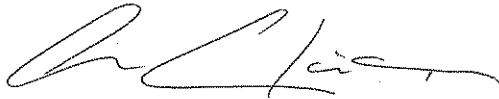
To the extent that Parliament chooses to rely on provincial and territorial privacy commissioners to perform *post facto* review of warrantless access to subscriber information, it follows that the federal government must commit to working with provincial and territorial governments to ensure that all of the relevant privacy commissioners have sufficient powers and resources. In this regard, please note that I have written two letters to Ontario's Attorney General, asking that the Ontario government play its part in these important law reform and oversight-related issues. Copies of those letters are attached.

Conclusion

The surveillance regime being put forward is aimed at capturing the full range of content, communication and traffic data associated with digital communications. As communication services continue to evolve, the legislation will empower the state to develop, update and enforce regulations directly aimed at shaping the technological capacities of telecommunication services so as to ensure that Web 2.0, 3.0 etc. communications can be readily intercepted, isolated and accurately correlated. In this context, it is reasonable to foresee that it will be much easier for the state to subject more individuals, including innocent individuals, to unwanted surveillance and scrutiny.

This debate is not about maintaining the state's surveillance capabilities, but trying to determine the proper balance in the evolving information age. In the face of so many significant changes, with so much at stake, and with so much left to regulation and implementation by policy, we are concerned that the public, Parliament and industry will be hard pressed to keep abreast of the technological challenges, the financial costs, and the invasiveness of an *expanding surveillance regime*. It is essential that Parliament and the public be well informed on technological, legal, regulatory and financial issues. The implications for privacy and other human rights must also be fully addressed, by providing for the necessary transparency, accountability and oversight. No less than the future of privacy – the future of freedom, is at stake.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Ann Cavoukian', written in a cursive style.

Ann Cavoukian, Ph.D.
Commissioner

Enclosures (2)

c: The Honourable John Gerretsen, Attorney General of Ontario
William Baker, Deputy Minister, Public Safety Canada
Myles Kirvan, Deputy Minister of Justice & Deputy Attorney General of Canada
Murray Segal, Deputy Attorney General of Ontario



Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

VIA EMAIL AND COURIER

October 24, 2011

The Honourable John Gerretsen
Attorney General of Ontario
Ministry of the Attorney General
McMurtry-Scott Building
720 Bay Street, 11th Floor
Toronto, ON M7A 2S9

Dear Minister Gerretsen:

I am writing to congratulate you on your appointment as the Attorney General of Ontario. While I have enjoyed a good working relationship with you in your previous Ministry, I look forward to working with you in your new capacity. In this regard, I think we may both benefit from an opportunity to meet briefly in person, perhaps early in the new year. If you are interested, my office will be in contact with yours to confirm a date and time.

In addition, I attach a copy of my September 23rd, 2011 letter to Minister Bentley, with whom my office also enjoyed a productive relationship, regarding section 20 of Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act (ECA)*. While this and two other related bills died on the Order Paper at the end of Parliament, I understand that the federal government intends to re-introduce all three shortly, in essentially the same format.

Over the last few weeks, public dismay about the likely re-introduction of Bills C-50, C-51, and C-52 has been growing. Many of the grave concerns that I and other privacy commissioners have had about these proposals were reflected in the October 22nd, 2011 article in the National Post, *Laws for 21st century: A guide to Canada's proposed cyber investigation bills* (copy attached).

Read together, their enactment would substantially diminish the privacy rights of Canadians. They would do so by enhancing the capacity of the state to conduct surveillance, as well as access private information, while reducing the frequency and vigour of judicial scrutiny, thus making it easier for the state to subject more individuals to expanded surveillance and scrutiny.

My concerns about these legislative proposals can be summarized as follows:

- The proposed surveillance powers come at the expense of the necessary privacy protective constitutional balance. In order to maintain that crucial balance, the federal government must be persuaded to acknowledge the sensitivity of traffic data, stored data, and tracking data and to re-draft the bills accordingly.

.../2



2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

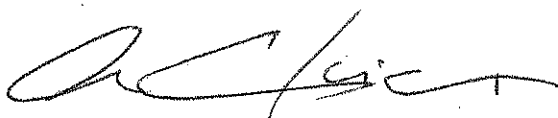
Tel: 416-326-3333
1-800-387-0073
Fax/Télé: 416-325-9195
TTY: 416-325-7539
www.ipc.on.ca

- Intrusive proposals require matching legislative safeguards. The courts, affected individuals, future Parliaments, and the public must be well informed about the scope, effectiveness, and deleterious effects of intrusive powers. If the federal government pushes ahead with expansive new surveillance powers, I hope you will join me in urging the federal government to publically commit to enacting the necessary oversight legislation, in tandem.
- Even with matching oversight, the proposed surveillance and access powers require more stringent conditions precedent.
- Entrenching a mandatory surveillance capacity regime on the public and its telecommunications service providers (TSP) must not go forward without adequate safeguards to protect the future of privacy and freedom; a comprehensive cost-benefit analysis, made publicly available, should precede rather than follow the making of so many significant public policy decisions. Public Parliamentary hearings should also be scheduled to ensure that civil society, as well as industry, have a full opportunity to provide substantial input on all of the bills, including the *ECA*.
- The proposal for warrantless access to subscriber information is untenable and should be totally withdrawn. It remains our view that the *ECA* should be amended to require that the provisions setting out TSP obligations concerning "subscriber information" be deleted and replaced with a court supervised regime.

While I continue to have the specific concerns about the focused legal and fiscal issues outlined in my September 23rd letter, I believe it is increasingly important for you to be aware of the *overarching* surveillance and access proposal and the serious implications it has for the privacy rights of the residents of Ontario as a whole.

Once again, congratulations on your appointment. I wish you every success in the important work ahead.

Sincerely yours,



Ann Cavoukian, Ph.D.
Commissioner

Enclosure



Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

September 23, 2011

VIA EMAIL AND LETTER MAIL

The Honourable Chris Bentley
Attorney General of Ontario
Ministry of the Attorney General
McMurtry-Scott Building
720 Bay Street, 11th Floor
Toronto, ON
M7A 2S9

Dear Minister Bentley:

I am writing you in relation to a single aspect of the federal government's anticipated package of surveillance-related legislation. My concerns focus on the legal and fiscal factors likely to undermine my capacity to fulfil the role the federal government purports to assign to my office under section 20 of Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act* (hereafter referred to as the *Electronic Communications Act* or *ECA*). While this bill died on the Order Paper at the end of the last Parliament, I understand that the federal government may re-introduce it in essentially the same form shortly.

In addition to providing the state with substantial control over the design and operation of "telecommunication service providers" (TSP) systems, the *Electronic Communications Act* would provide law enforcement and CSIS officials with warrantless access to *subscriber information* for the purposes of performing any of their duties or functions. *Subscriber information* includes a named individual's IP address or mobile ID number or the name and contact information of a subscriber associated with an IP address or mobile ID number.

Access to TSP-held *subscriber information* will empower police to link specific communication devices with particular individuals, as well as to monitor a wide range of their communications and activities in cyberspace. Since this power would be available for the purposes of performing *any* police duties or functions, the potential benefits and risks will be comparably wide ranging.

Section 20 of the *ECA* provides for attenuated *post facto* review of warrantless access to subscriber information. In doing so, it relies on provincial and territorial privacy commissioners and ombudsmen ("public officers" or "privacy officers") to: (i) conduct audits to assess local and provincial police compliance with provisions of the Bill that broadly empower the collection and use of subscriber information; and (ii) review police reports generated after police determine that something has occurred with respect to their own exercise of these access powers that, in their opinion, ought to be brought to the attention of the responsible provincial minister (in Ontario, the Attorney General).

.../2



Legal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services juridiques
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléco: 416-325-9186
TTY: 416-325-7539
www.ipc.on.ca

Under section 20(6) of the *ECA*, the Privacy Commissioner of Canada must provide Parliament with an annual report identifying the provincial privacy officers who may receive any such opinion-based reports and the powers that they have to conduct section 20 compliance audits.

In my case, I lack the powers necessary to fulfill the proposed duties. In fact, under our home statutes, I do not have any audit powers. This may be the case for other provincial and territorial officers. This concern was reflected in a letter of March 9, 2011 signed by all the federal, provincial and territorial privacy officers. In that letter, we joined our colleagues in calling on the federal government to commit to working with provincial and territorial governments to ensure that all of our offices have sufficient powers and resources should the *Electronic Communications Act* be enacted. It does not appear that any such commitment has been forthcoming.

As I am sure you will agree, under these circumstances, the federal government's approach to oversight is clearly untenable. Quite apart from the constitutional issues raised by the enactment of a regime of warrantless access, it is noteworthy that in some circumstances, aspects of *post facto* oversight of communications-related surveillance powers have been found to be constitutionally required (see, for example *R. v. Six Accused Persons*, [2008] B.C.J. No. 293] and *R. v. Riley*, [2008] O.J. No. 2887). In addition, the audit duties to be imposed on my office under section 20 may raise division of powers problems.

Finally, I note that I would lack the necessary fiscal and human resources required to adequately perform the legislative duties imposed under the *Electronic Communications Act*.

While it continues to be our view that the *Electronic Communications Act* should be amended to ensure that police access to *subscriber information* is subject to a system of prior judicial authorization, it appears likely that the federal government will move ahead with a system of warrantless access and attenuated *post facto* review.

In this context, I wanted to alert you to the federal government's apparent failure to account for these significant problems and to urge you to raise these matters with your federal counterparts. Should they insist on proceeding in this direction, you may be faced with having to address uninvited legislative, fiscal, and constitutional issues.

Please do not hesitate to contact me if you wish to discuss these matters further.

Sincerely yours,



Ann Cavoukian, Ph.D.
Commissioner

cc: Murray Segal, Deputy Minister