CHAPTER VIII

Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era

Michael Geist

Introduction

Months of surveillance-related leaks from US whistle-blower Edward Snowden have fuelled an international debate over privacy, spying, and Internet surveillance. The leaks have painted a picture of ubiquitous surveillance that captures "all the signals all the time," sweeping up billions of phone calls, texts, e-mails, and Internet activity with dragnet-style efficiency.

In the United States, the issue has emerged as a political concern, leading to promises from US President Barack Obama to more carefully circumscribe the scope of US surveillance programs.[1] Moreover, US telecom and Internet companies have also responded to political and customer pressure. Verizon[2] and AT&T,[3] two US telecom giants, have begun issuing regular transparency reports on the number of law enforcement requests they receive for customer information. The telecom transparency reports come following a similar trend from leading Internet companies such as Google, Twitter, Microsoft, and Facebook.

While the United States gradually grapples with the Snowden fallout, the Canadian response has been muted at best. Canadian government officials have said little about Canadian surveillance activities, despite revelations of spying activities in Brazil, capturing millions of Internet downloads daily, surveillance of airport wireless networks, cooperation with foreign intelligence agencies,[4] a federal court decision

that criticized Canada's intelligence agencies for misleading the court, and a domestic metadata program that remains largely shrouded in secrecy. Canadian telecom companies such as Rogers and Telus[5] reluctantly followed their US counterparts in issuing transparency reports in 2014,[6] though Bell (the largest provider) remains a holdout and reports indicate that government officials expressed concern about any public reporting.[7] In fact, the Canadian government seems to have moved in the opposite direction, by adopting a lower threshold for warrants seeking metadata than is required for standard warrants in Bill C-13, a cyberbullying and lawful access bill that passed the House of Commons in October 2014.[8] Further, in January 2015, the government introduced Bill C-51, the *Anti-Terrorism Act, 2015*, which greatly expands information sharing between Communications Security Establishment (CSE), Canadian Security Intelligence Service (CSIS), and fifteen other government departments and agencies.[9]

As the leaks continue — journalist Glenn Greenwald has indicated that there is more Canadian-related information forthcoming[10] — Canadians are likely to demand greater transparency and accountability about government surveillance activities.[11] Should the issue emerge as a political liability, the question that this chapter examines is where the emphasis should lie. It argues that while the instinctive response may be to focus on improved oversight and accountability mechanisms,[12] the bigger challenge will be to address the substantive shortcomings of the current Canadian legal framework. Indeed, improved oversight without addressing the limitations within current law threatens to leave many of the core problems in place. In short, watching the watchers is not enough.

Background

The US role in global surveillance has unsurprisingly captured the lion's share of attention, yet Canada's participation — both as a member of the "Five Eyes" group of countries that includes the United States, the United Kingdom, Australia, and New Zealand, and as a country with an an active domestic and international surveillance program — merits closer examination.[13] Several statutes govern the scope of Canadian activities.

The *National Defence Act* governs the Canadian Security Establishment (CSE), which operates Canada's signals intelligence activities.[14] It limits the CSE mandate to the following three activities:

(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
(b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.[15]

This mandate was developed in the aftermath of the 11 September 2001 attacks in the United States. The Act further restricts the activities carried out under parts (a) and (b) by stating that they

(a) shall not be directed at Canadians or any person in Canada; and
(b) shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.[16]

The CSE commissioner has characterized the limitations on parts (a) and (b) of the CSE mandate in the following manner:

> CSEC [CSE] is prohibited from directing its foreign signals intelligence collection and IT security activities at Canadians, regardless of their location anywhere in the world, or at any person in Canada, regardless of their nationality;
> In conducting these activities, CSEC may unintentionally intercept a communication that originates or terminates in Canada in which the originator has a reasonable expectation of privacy, which is a "private communication" as defined by the *Criminal Code*. CSEC may use and retain a private communication obtained this way but only if it is essential to either international affairs, defence or security, or to identify, isolate or prevent harm to Government of Canada computer systems or networks; and
> To provide a formal framework for the unintentional interception of private communications while conducting foreign signals

> intelligence collection or IT security activities, the *National Defence Act* requires express authorization by the Minister of National Defence. These are known as ministerial authorizations. The Minister may authorize the activities once he or she is satisfied that specific conditions provided for in the Act have been met, which includes assurances of how such unintentional interceptions of private communications would be handled should they arise.[17]

The government has unsurprisingly defended CSE and consistently claimed that its activities are compliant with the law. In seeking to assure Canadians that there are appropriate safeguards, Justice Minister Peter MacKay told the House of Commons in 2013, "This program is specifically prohibited from looking at the information of Canadians. This program is very much directed at activities outside the country, foreign threats, in fact. There is rigorous oversight. There is legislation in place that specifically dictates what can and cannot be examined."[18]

When asked specifically about the Snowden leaks and the revelations of US surveillance programs, MacKay responded

> I would point him, again, to the fact that CSE does not target the communications of Canadians. This is foreign intelligence. This is something that has been happening for years. In fact, as I said, the commissioner highlighted that the "activities were authorized and carried out in accordance with the law, ministerial requirements, and CSEC's policies and procedures.[19]

Notwithstanding the minister's assurances, there have been mounting calls for greater oversight and accountability in response to the Snowden revelations and Canada's participation in global surveillance activities. Those calls increased following the introduction of Bill C-51, which expanded CSIS powers without enhancing related oversight.[20] There is a CSE commissioner who issues annual reports and has been increasingly vocal about his oversight role.[21] Yet, despite the existence of an independent commissioner, many believe that more is needed. For example, University of Toronto professor Ron Deibert has argued that "The Canadian checks and balances just aren't there. We have no parliamentary oversight of CSEC, no adequate independent entity to watch the watchers and act as a

constraint on misbehaviour. It just doesn't exist now."[22] Deibert's view is widely shared, with many experts (including some in this volume) pointing to the need for more robust review and oversight to provide Canadians with better assurances that the operation of surveillance programs are compliant with the law.

In fact, there have been repeated attempts at improving oversight, with particular attention paid to the role of parliamentarians.[23] In 2005, Bill C-81, *An Act to Establish the National Security Committee of Parliamentarians*, was introduced in the House of Commons.[24] The bill, which did not proceed past first reading, would have established new oversight powers for a committee comprised of members of Parliament. More recently, Liberal MP Wayne Easter sought to revive the bill in Bill C-551, a private members' bill.[25] In June 2014, Liberal MP Joyce Murray introduced Bill C-622, a CSE accountability and transparency bill.[26]

Oversight and accountability are certainly crucial issues and efforts to enhance the current model, which relies heavily on the CSE commissioner, should be pursued vigorously. However, the danger with focusing chiefly on stronger oversight is that the statutory framework governing CSE necessarily limits the review. In other words, reviews of agencies governed by laws that may permit privacy-invasive activities or that fail to establish a suitable level of oversight in order to engage in certain activities is doomed from the start.

Even if the CSE commissioner were fully empowered to review and publicly document concerns associated with CSE (which some critics doubt), substantive concerns within the legal framework might still go unaddressed. Therefore, this chapter argues that improved oversight without legal reforms is unlikely to address the broader public concerns about lawful surveillance activities that may extend beyond public expectations about the privacy of network communications.

Substantive Concerns With the Current Legal Framework

Metadata

The legality of surveillance programs that capture metadata sits at the heart of much of the legal debate in both the United States and Canada. Metadata — data about data — is information that is automatically generated by the use of communications devices and services such as cellphones, Internet browsing, and text messaging. The

metadata may include information on the time of the communication, the parties to the communication, the devices used to communicate, and the location of the communication.[27]

In the United States, the NSA inspector general under the Clinton administration concluded in 1999 that searching telephone metadata constituted unauthorized surveillance:

> NSA proposed that it would perform contact chaining on metadata it had collected. Analysts would chain through masked U.S. telephone numbers to discover foreign connections to those numbers, without specifying, even for analysts, the U.S. number involved. In December 1999, the Department of Justice (DoJ), Office of intelligence Policy Review (OIPR) told NSA that the proposal fell within one of the FISA definitions of electronic surveillance and, therefore, was not permissible when applied to metadata associated with presumed U.S. persons (i.e., U.S. telephone numbers not approved for targeting by the FISC).[28]

Yet, in the aftermath of the September 11 attacks, the US approach to the question changed.[29] The United States began to collect metadata, with the Foreign Intelligence Surveillance Court (FISC) ordering telecom companies in 2006 to provide the NSA with "comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, communications device identifier, and so forth), trunk identifier, and time and duration of call."[30] The legality of the US program has been the subject of conflicting court decisions and seems likely to be headed to the US Supreme Court.

While details on the Canadian metadata programs remain secret, there is little doubt that Canadian intelligence agencies are engaged in capturing metadata, much like their US counterparts.[31] The *Globe and Mail* reported in 2013 that a secret Canadian metadata surveillance program was first launched in 2005 under then-Prime Minister Paul Martin by Defence Minister Bill Graham, only to be stopped in 2008 amid privacy concerns. The program was restarted in 2011 with new rules.[32] The details of the program have never been publicly disclosed and the legal questions about the privacy protections granted to metadata collection remain unanswered.

There is reason to believe that CSE believes that metadata is not subject to the privacy protections accorded to content. In 2007,

then-CSE chief John Adams told the Standing Senate Committee on National Security and Defence, "What is your interpretation of intercept, if I were to ask? If you asked me, it would be if I heard someone talking to someone else or if I read someone's writing. An intercept would not be to look on the outside of the envelope. That is not an intercept to me."[33] The reference to "outside of the envelope" would appear to be a reference to metadata.

Assurances that metadata surveillance is less invasive than tracking the content of telephone calls or Internet usage also ring hollow. Metadata can include geolocation information, call duration, call participants, and Internet protocol addresses. While officials suggest that this information is not sensitive, there are many studies that have concluded otherwise. These studies have found that metadata alone can be used to identify specific persons, reveal locational data, or even disclose important medical and business information.

For example, a Stanford study found that researchers could predict romantic relationships automatically using only phone metadata, while an MIT study that examined months of anonymized cellphone data and found that only four data points were needed to identify a specific person 95 per cent of the time.[34] Other studies have found that sexual identity can be guessed based on Facebook metadata.[35]

Canadian privacy commissioners have also highlighted the privacy implications of metadata and information that is not typically classified as "content." The Privacy Commissioner of Canada released a report on the privacy value of IP addresses in 2012, noting that one data point could lead to information on website habits that includes sites on sexual preferences.[36] Former Ontario Privacy Commissioner Ann Cavoukian has issued a primer on metadata that finds that it may be more revealing than content.[37]

The Supreme Court of Canada echoed similar concerns with privacy and metadata in *R. v. Vu*. The court specifically discussed the privacy importance of computer-generated metadata, noting that

> most browsers used to surf the Internet are programmed to automatically retain information about the websites the user has visited in recent weeks and the search terms that were employed to access those websites. Ordinarily, this information can help a user retrace his or her cybernetic steps. In the context of a criminal investigation, however, it can also enable investigators to access intimate details about a user's interests, habits, and

> identity, drawing on a record that the user created unwittingly: O. S. Kerr, "Searches and Seizures in a Digital World" (2005), 119 Harv. L. Rev. 531, at pp. 542–43. This kind of information has no analogue in the physical world in which other types of receptacles are found.[38]

In fact, even CSE apparently acknowledged in 2008 that "bulk, unselected metadata presents too high a risk to share with second parties at this time, because of the requirement to ensure that the identities of Canadians or persons in Canada are minimised, but re-evaluation of this stance is ongoing."[39]

This position is consistent with US expert positions on the value of metadata. General Michael Hayden, former director of the NSA and the CIA has stated, "we kill people based on metadata."[40] Stewart Baker, former NSA general counsel, has said, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."[41]

A recent US court brief signed by some of the world's leading computer experts notes

> Telephony metadata reveals private and sensitive information about people.
> It can reveal political affiliation, religious practices, and people's most intimate associations. It reveals who calls a suicide prevention hotline and who calls their elected official; who calls the local Tea Party office and who calls Planned Parenthood. The aggregation of telephony metadata — about a single person over time, about groups of people, or with other datasets — only intensifies the sensitivity of the information.[42]

Despite the studies on the implications of metadata, the Canadian legal framework downplays the privacy import of such information.[43] As noted above, government officials have dismissed metadata collection as relatively insignificant when questioned about the practice.

In fact, the government recently created a specific warrant for law enforcement designed to obtain metadata with a lower threshold than that used for other sensitive information, such as content. Bill C-13, the lawful access/cyberbullying bill which took effect in March 2015, establishes a definition for transmission data 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; (c) does not reveal the substance, meaning or purpose of the communication.[44]

The bill created a new warrant that allows a judge to order the disclosure of transmission data where there are reasonable grounds to suspect that an offence has been or will be committed, the identification of a device or person involved in the transmission will assist in an investigation, or will help identify a person. The government relied on the fact that this is a warrant with court oversight to support the claim that Canadians should not be concerned by this provision. Yet the reality is that there is reason for concern, as the implications of treating metadata as having a low privacy value is enormously troubling. Given the level of privacy interest with metadata, many argued that the higher, "reasonable grounds to believe" standard should have been adopted in the Bill C-13 transmission data warrant provision.[45] The government rejected those submissions and passed the bill in the House of Commons in October 2014.

Without addressing the privacy implications of metadata, reforms to the accountability mechanisms built into Canada's surveillance frameworks are destined to fall short. The Canadian approach to metadata reflects an outdated perspective that minimizes its privacy importance. Those views have played a crucial role in increasing the collection of metadata, while simultaneously adopting lower standards of legal safeguards over its collection and use. With a broad-based ministerial authorization on metadata collection seemingly establishing few limits, the metadata program now represents one of the most significant privacy-related concerns with Canadian surveillance practices.

The solution must therefore lie in developing policies that better reflect the privacy implications of metadata collection. A public review of the metadata authorization is long overdue, accompanied

by a closer examination of potential limitations and oversight that can be adopted as part of any bulk metadata collection program. Moreover, the use of lower warrant thresholds for metadata collection (referred to in the legislation as transmission data) should be revisited with standards adopted that recognize the privacy equivalency of the metadata of a communication and the content of the communication itself. Absent a significant overhaul of the Canadian approach to metadata collection, improved oversight of surveillance activities will only guarantee that reviews are unable to fully address the privacy implications of the Canadian legal framework.

The Blurring of Jurisdiction

One of the most important distinctions within the current CSE legal framework is the stipulation that foreign intelligence activities "shall not be directed at Canadians or any person in Canada." The distinction between foreign collection of information (which is permitted by the statute) and domestic collection (which is not) is regularly cited as a clear line of demarcation between legal and illegal surveillance activities.[46] Indeed, CSE's own explanation of its activities states

> CSE's mandate involves the collection of foreign signals intelligence and the protection of the computer systems and networks of the Government of Canada from mischief, unauthorized use and interference. When fulfilling either of these mandates, CSE does not direct its activities at Canadians, Canadians abroad or any persons in Canada. In fact, CSE is prohibited by law from directing its activities at Canadians anywhere or at anyone in Canada.[47]

Yet, despite the repeated assurances, the commingling of data through integrated communications networks and "borderless" Internet services residing on servers around the world suggests that distinguishing between Canadian and foreign data seems like an outdated and increasingly impossible task. In the current communications environment, tracking Canadians seems inevitable and makes claims that such domestic surveillance is "inadvertent" increasingly implausible.

The extensive US surveillance programs appear to capture just about all communications: everything that enters or exits the United States, anything involving a non-US participant, and anything that

travels through undersea cables. This would seem to leave Canadian cellphone and Internet users at a similar risk of surveillance regardless of the nationality of the carrier and suggests that Canadian companies may be facilitating surveillance of their customers by failing to adopt safeguards that render it more difficult for foreign agencies to access data.

For example, both Bell and Rogers link their e-mail systems for residential customers to US giants: Bell is linked to Microsoft and Rogers is linked to Yahoo. In both cases, the inclusion of a US e-mail service provider may allow for US surveillance of Canadian e-mail activity. While the Canadian privacy commissioner previously dismissed concerns associated with using US e-mail providers on the grounds that Canada had similar security laws,[48] the new surveillance revelations suggest that a re-examination of that conclusion may be warranted.

As further analyzed in Clement and Obar's chapter, the issue of avoiding US routing is particularly important, since even Canadian domestic communications that travel from one Canadian location to another may still transit through the United States and thus be captured by US surveillance. Despite these risks, Bell requires other Canadian Internet providers to exchange Internet traffic outside the country at US exchange points, ensuring that the data is potentially subject to US surveillance. In fact, some estimate that 90 per cent of Canadian communications traffic transits through the United States.[49] Moreover, with the regular surveillance demands for the e-mail traffic that passes through Blackberry's Waterloo-based servers and the likely interception of communications traffic through several undersea cables that enter Canada, there is little doubt that Canadian Internet and phone use is subject to significant US surveillance activity.[50]

While the current surveillance statutes may have been developed in a world where geography mattered, the communications borders have been largely blurred, leaving a North American communications network that has little regard for national boundaries. Canadian law is therefore increasingly unable to provide credible assurances about the limits of domestic collection.

Given the global nature of the surveillance activities and the likely commingling of Canadian data (even in instances where CSE activities are not directed toward the country or Canadians), revisiting the jurisdictional issues associated with CSE is essential. As with the need for a review of metadata collection that better reflects

current technologies, an examination of the jurisdictional limits of CSE activities premised on modern communications networks is needed. The Canadian government may determine that the jurisdictional limits on CSE should be revisited and expanded. In such a case, the statute should better reflect those limits, rather than maintaining the fiction that CSE surveillance can be neatly divided between domestic and foreign-based activities.

Data and Intelligence Information Sharing

Data and intelligence information sharing is an important part of modern intelligence activities. Indeed, the prospect that US surveillance becomes a key source for Canadian agencies, while Canadian surveillance supports US agencies, does not strike anyone as particularly far-fetched. Wayne Easter, a former government minister with responsibility for CSIS, has said that such sharing is common.[51] In other words, relying on the domestic–foreign distinction is necessary for legal compliance, but does not provide much assurance to Canadians that they are not being tracked.

In fact, Bill C-51 would greatly expand potential information sharing practices. The bill includes the *Security of Canada Information Sharing Act* (SCISA), a bill within the bill, that permits information sharing across government for an incredibly wide range of purposes, most of which have nothing to do with terrorism. The government has tried to justify the provisions on the grounds that Canadians would support sharing information for national security purposes, but the bill allows sharing for reasons that would surprise and disturb most Canadians.[52] Moreover, the scope of sharing is exceptionally broad, covering seventeen government institutions, with government granting itself the right to expand sharing to other departments.[53] In fact, the bill notes that further use and disclosure may occur in accordance with the law."[54]

Canadian Laws That Harmonize Information Sharing

Law enforcement agencies in Canada and the United States currently employ a harmonized approach to sharing information related to cross-border crime, terrorist activity, and immigration matters. For example, a post-9/11 agreement between Canada and the United States established a thirty-point action plan for creating a secure border.[55] Moreover, integrated intelligence is one of eight

objectives oriented towards joint data sharing and intelligence coordination. Canada has also established Integrated National Security Enforcement Teams (INSETs) to fight terrorist threats.[56] INSETs include representatives from federal enforcement and intelligence agencies, as well as US law enforcement agencies on a case-by-case basis. The federal government has identified increased joint antiterrorism efforts as a priority.[57]

Information-sharing instruments are also used to obtain information relating to financial investigations. For example, the US Securities and Exchange Commission (SEC) has Memorandums of Understanding (MOUs) with foreign securities regulators to cooperate and share information on the regulation of the financial industry.

Several Canadian statutes specifically authorize cross-border information transfers. The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* authorizes the Financial Transactions and Reports Analysis Centre of Canada to share financial information related to the goal of preventing money laundering and terrorist financing.[58] The *Department of Immigration and Citizenship Act* includes a provision that allows the minister to implement agreements with foreign governments in order to facilitate the coordination of policies for which he or she is responsible.[59]

The active connection between Canadian and US officials moved to the forefront with reports that Canadian officials may have played a starring role in facilitating US efforts to create a "backdoor" to widely used encryption standards. The Canadian role in these developments is linked to how the NSA managed to gain control over the standard setting process. In 2006, CSE ran the global standard setting process for the International Organization for Standardization. The NSA convinced CSE to allow it to rewrite an earlier draft and ultimately become the sole editor of the standard.

CSE claims that its relationship with the NSA during the standard setting process was merely designed to support the Canadian government's effort to secure its technological infrastructure. However, it is now clear that Canada worked with the United States to ensure that the backdoor was inserted into the encryption standard and that it may have gained access to decryption information in the process.

Given common threats, few doubt the importance of information sharing. Yet differing privacy laws raise serious concerns about

whether personal information collected in Canada receives the same level of protection once it is provided to foreign intelligence agencies. Conducting effective reviews of data protection and policies that are outside of the physical control of Canadian agencies represents a significant challenge. Moreover, oversight and accountability mechanisms are largely limited to domestic reviews. Without an oversight mechanism capable to assessing the status of Canadians subject to information sharing practices, providing appropriate protection relies upon broader legal and contractual structures that govern the use of shared data. A review of those structures in an environment where data may flow freely between agencies is needed.

Federal Court Concerns

The Federal Court of Canada has also expressed concern about inappropriate data sharing activities. In 2013, Justice Richard Mosley, a federal court judge, issued a stinging rebuke to Canada's intelligence agencies and the Justice Department, ruling that they misled the court when they applied for warrants to permit the interception of electronic communications.[60] While the government has steadfastly defended its surveillance activities by maintaining that it operates within the law, Justice Mosley, a former official with the Justice Department who was involved with the creation of the *Anti-Terrorism Act*, found a particularly troubling example where this was not the case. Mosley's concern stemmed from warrants involving two individuals that were issued in 2009 permitting the interception of communications both in Canada and abroad using Canadian equipment. At the time, the Canadian intelligence agencies did not disclose that they might ask their foreign counterparts to intercept the foreign communications.

In June 2013, the CSE commissioner issued his annual report, which included a cryptic recommendation that the agency "provide the Federal Court of Canada with certain additional evidence about the nature and extent of the assistance CSE may provide to CSIS."[61] That recommendation caught Mosley's attention, and he ordered the CSE and CSIS to appear in court to disclose if the recommendation was linked to the warrants he had issued and discuss whether the additional evidence might have had an impact on the decision to grant the warrants in the first place.

It turned out that the additional evidence — which involved several warrants, including those issued by Mosley — was indeed the

fact that CSE was tasking foreign agencies to conduct interceptions on its behalf. Based on the new submissions, Mosley concluded that Canadian intelligence agencies strategically omitted disclosing the information as they admitted that the evidence provided to the court "was 'crafted' with legal counsel to exclude any reference to the role of the second parties."[62]

The failure of Canada's intelligence agencies to meet their legal obligations of full and frank disclosure raises serious questions about the adequacy of oversight over Canada's surveillance activities. When concerns were raised in 2013 about the activities, then-Defence Minister Peter MacKay assured the public that there is "rigorous" oversight and that all aspects of the programs were carried out in compliance with the law.

The federal court ruling raised real doubt about the validity of those assurances. Indeed, there are lingering questions about both the impartiality of Justice lawyers who provided advice to "craft evidence" and the ability of the federal court to serve as a key oversight mechanism for Canadian surveillance, particularly when some programs do not require court approval and reports from the CSE commissioner have faced lengthy delays.

Rather than addressing these concerns directly, in October 2014, days after an attack on Parliament Hill, the government introduced Bill C-44, the *Protection of Canada from Terrorists Act*.[63] The bill seeks to address the Mosley decision by removing territorial restrictions on CSIS. The bill includes clauses that state that CSIS may conduct investigations within or outside Canada and seek a warrant to allow foreign investigations. Moreover, it opens the door to warrants that apply outside the country regardless of the law in Canada or elsewhere. It provides, "Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize activities outside Canada to enable the Service to investigate a threat to the security of Canada."[64]

This is a remarkably broad provision, as it allows the federal court to issue warrants that violate the laws of other countries, including foreign privacy laws. The bill was passed through committee review within a matter of weeks. Bill C-44 may reverse the Mosley decision, but what it does not do is address ongoing concerns regarding the accountability and transparency of Canada's security intelligence agencies.[65] Indeed, the Mosley case in particular raised troubling questions about the adequacy of oversight over Canada's

surveillance activities. Rather than address those concerns, the government has instead simply reversed the court rulings through legislative reform, leaving the current inadequate oversight system untouched.

European Union Concerns

The likelihood of Canadian data sharing has also attracted the attention of foreign governments, most notably the European Parliament. In December 2013, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs has issued a draft report on US surveillance activities and its implications for European fundamental rights. The report brought Canada into the discussion, noting Canada's participation in the Five Eyes consortium and expressing concern about the implications for trust in the Canadian legal system. The report states

> whereas according to the information revealed and to the findings of the inquiry conducted by the LIBE Committee, the national security agencies of New Zealand and Canada have been involved on a large scale in mass surveillance of electronic communications and have actively cooperated with the US under the so called "Five eyes" programme, and may have exchanged with each other personal data of EU citizens transferred from the EU;
> whereas Commission Decisions 2013/651 and 2/2002 of 20 December 2001 have declared the adequate level of protection ensured by the New Zealand and the Canadian Personal Information Protection and Electronic Documents Act; whereas the aforementioned revelations also seriously affect trust in the legal systems of these countries as regards the continuity of protection afforded to EU citizens; whereas the Commission has not examined this aspect.[66]

As a result of the concerns with Canadian surveillance, the report recommends a re-examination of the adequacy finding of Canadian privacy law:

> Calls on the Commission and the Member States to assess without delay whether the adequate level of protection of the New

> Zealand and of the Canadian Personal Information Protection and Electronic Documents Act, as declared by Commission Decisions 2013/651 and 2/2002 of 20 December 2001, have been affected by the involvement of their national intelligence agencies in the mass surveillance of EU citizens and, if necessary, to take appropriate measures to suspend or reverse the adequacy decisions; expects the Commission to report to the European Parliament on its findings on the above mentioned countries by December 2014 at the latest;[67]

European concerns with Canadian privacy practices arose again in November 2014 as the European Parliament voted to send a Canada–European Union data-sharing agreement on airline passenger name records to the European Court of Justice for further review. The review, which may not be completed for several years, seeks to ensure that the agreement is compliant with European Union treaties and with the *EU Charter of Fundamental Rights*.[68]

The recent revelations and court cases point to the need for a comprehensive review of Canada's role within Five Eyes and a greater understanding of data sharing and intelligence-gathering activities between intelligence agencies. Without such a review and potential reforms, claims that Canadian agencies operate within the law will provide only limited comfort to those concerned with surveillance that falls outside the current statutory framework.

The European responses to Canadian surveillance and privacy practices point to the risks associated with the current activities, since failure to adequately address the privacy implications of Canadian surveillance activities could hamper Canada's ability to conclude data sharing agreements with other governments or create restrictions on data transfers between Canada and other jurisdictions.

Limited Privacy Protections under Canadian Law

While Canadians often point to the existence of private sector privacy legislation as evidence that there are protections that do not exist under US law (which has not implemented a broadly applicable privacy statute for the private sector), the reality is that Canadian law currently affords limited protections as part of law enforcement or national security investigations. The exceptions within the law become particularly problematic given the increasingly important

role of private sector companies such as telecom and Internet companies in the collection and disclosure of their communications activities.

The *Personal Information Protection and Electronic Documents Act (*PIPEDA*)* establishes the obligations of private organizations with regard to the data they collect in the course of commercial activity.[69] Unless subject to a substantially similar provincial law, the Act applies to every private-sector organization in Canada that collects, uses, or discloses personal information.[70]

PIPEDA includes several exceptions for disclosure of personal information without knowledge or consent. Section 7(3)(c) enables an organization to disclose personal information where it is required "to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information."[71]

Domestic Disclosures

For many years, government, law enforcement, and telecom providers pointed to PIPEDA and the perceived limited privacy import of subscriber information to argue that it could be disclosed without a warrant. In 2014, the issue began to attract increasing attention, leading to disclosures that placed the spotlight on widespread warrantless access to subscriber information.

In 2011, the Privacy Commissioner of Canada sent letters to the twelve biggest Canadian telecom and Internet providers seeking information on their disclosure practices. Rogers, Bell, and RIM proposed aggregating the information to keep the data from individual companies secret. The response dragged on for months, with Bell admitting at one point that only four providers had provided data and expressing concern about whether it could submit even the aggregated response since it would be unable to maintain anonymity. The companies ultimately provided aggregated information revealing that, in 2011, there were 1,193,630 requests, the majority of which were not accompanied by a warrant or court order. The data indicates that telecom and Internet providers gave the government what it wanted: three providers alone disclosed information from 785,000 customer accounts.[72]

Those revelations, which only came to light in 2014, were preceded by NDP MP Charmaine Borg's effort to obtain information on government agencies' requests for subscriber data. While many

agencies refused to disclose the relevant information, Canada Border Services Agency (CBSA) revealed that it had made 18,849 requests in one year for subscriber information including geolocation data and call records. The CBSA obtained a warrant in 52 instances with all other cases involving a simple request without court oversight. The telecom and Internet providers fulfilled the requests virtually every time — 18,824 of 18,849 — and the CBSA paid a fee of between one dollar and three dollars for each request.[73]

In fact, the CBSA revelations follow earlier information obtained under the *Access to Information Act* that in 2010 the RCMP alone made over 28,000 requests for subscriber information without a warrant. These requests go unreported — subscribers do not know their information has been disclosed and the Internet providers and telecom companies aren't talking either. In fact, according to a 2014 Privacy Commissioner of Canada audit, the RCMP itself maintains incomplete and inaccurate records of its requests.[74]

The disclosures also revealed that the telecom companies have established law enforcement databases that provide ready access to subscriber information in a more efficient manner. For example, the Competition Bureau reports that it "accessed the Bell Canada Law Enforcement Database" twenty times in 2012–2013.

The absence of court oversight may surprise many Canadians, but the government has long actively supported the warrantless disclosure model. In 2007, it told the Privacy Commissioner of Canada that an exception found in the private sector privacy law to allow for warrantless disclosure was designed "to allow organizations to collaborate with law enforcement and national security agencies without a subpoena, warrant or court order."[75]

While the massive disclosure of subscriber information without court oversight garnered considerable attention, the practices may change due to the Supreme Court of Canada *R. v. Spencer* decision, released in June 2014.[76] The *Spencer* decision, which examined the legality of voluntary warrantless disclosure of basic subscriber information to law enforcement, called into question long-standing practices and forced law enforcement and other agencies to re-examine their approach.

In a unanimous decision written by Justice Thomas Cromwell, the court issued a strong endorsement of Internet privacy, emphasizing the privacy importance of subscriber information, the right to anonymity, and the need for police to obtain a warrant for subscriber

information except in exigent circumstances or under a reasonable law.

The court recognizes that there is a privacy interest in subscriber information. While the government has consistently sought to downplay that interest, the court finds that the information is much more than a simple name and address, particular in the context of the Internet. As the court states,

> the Internet has exponentially increased both the quality and quantity of information that is stored about Internet users. Browsing logs, for example, may provide detailed information about users' interests. Search engines may gather records of users' search terms. Advertisers may track their users across networks of websites, gathering an overview of their interests and concerns. Cookies may be used to track consumer habits and may provide information about the options selected within a website, which web pages were visited before and after the visit to the host website and any other personal information provided. The user cannot fully control or even necessarily be aware of who may observe a pattern of online activity, but by remaining anonymous — by guarding the link between the information and the identity of the person to whom it relates – the user can in large measure be assured that the activity remains private.[77]

Given all of this information, the privacy interest is about much more than just name and address.

Second, the court expands our understanding of informational privacy, concluding that there are three conceptually distinct issues: privacy as secrecy, privacy as control, and privacy as anonymity. It is anonymity that is particularly notable as the court recognizes its importance within the context of Internet usage. Given the importance of the information and the ability to link anonymous Internet activities with an identifiable person, a high level of informational privacy is at stake.

Third, not only is there a significant privacy interest, but there is also a reasonable expectation of privacy by the user. The court examined both PIPEDA and the Shaw terms of use (the ISP in the *Spencer* case) and concluded that PIPEDA must surely be understood within the context of protecting privacy (not opening the door to

greater disclosures) and that the ISP agreement was confusing at best and may support the expectation of privacy. With those findings in mind,

> in the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. The disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search.[78]

Fourth, having concluded that obtaining subscriber information was a search with a reasonable expectation of privacy, the information was unconstitutionally obtained, therefore led to an unlawful search. Addressing the impact of the PIPEDA voluntary disclosure clause, the court noted,

> Since in the circumstances of this case the police do not have the power to conduct a search for subscriber information in the absence of exigent circumstances or a reasonable law, I do not see how they could gain a new search power through the combination of a declaratory provision and a provision enacted to promote the protection of personal information.[79]

The *Spencer* decision placed the spotlight on longstanding, albeit but legally questionable, law enforcement and government agencies subscriber information request practices that were actively supported by Canadian telecom providers. While the decision may result in significant practice reforms, the uncertainty confirms that Canadian domestic privacy law does not provide strong safeguards against warrantless disclosures of subscriber information.

Foreign Disclosures

In addition to PIPEDA's weakness on domestic warrantless disclosures, the statute does not address whether foreign orders, such as those made by a Foreign Intelligence Surveillance Court (FISC) or a grand jury can be considered as made by "a court, person or body with jurisdiction to compel" so as to fall within another PIPEDA consent exception. The statute is silent on the jurisdictional distinction

making it possible that US orders validly made under US personal jurisdiction can be considered an exception.

Section 7(3)(c.1) permits disclosure without consent where the disclosure is made to a government institution where "(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law."[80] The inclusion of foreign laws within this exception indicates that disclosure for US counterterrorism investigations through national security letters or section 215 orders might qualify under the act's exceptions. The related issue is whether "government institution" is limited to a Canadian government institution or whether a foreign government institution could suffice. If the exception is limited to Canadian government institutions, US authorities would likely need to tender their requests for disclosure through CSIS or the Canadian Department of Justice to qualify.

The Privacy Commissioner of Canada has addressed these issues in a series of complaints involving the Canadian Imperial Bank of Commerce and the outsourcing of credit card processing to the United States.[81] While each complainant raised slightly different issues, all complainants primarily objected to the possible scrutiny of their personal information by US authorities within the context of foreign intelligence gathering.

With regard to the risk of disclosure to US authorities, the Commissioner noted,

> The possibility of U.S. authorities accessing Canadians' personal information has been raised frequently since the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001 (USA PATRIOT Act). Prior to the passage of this Act, U.S. authorities were able to access records held by U.S.-based firms relating to foreign intelligence gathering in a number of ways. What has changed with the passage of USA PATRIOT Act is that certain U.S. intelligence and police surveillance and information collection tools have been expanded, and procedural hurdles for U.S. law enforcement agencies have been minimized. Under section 215 of the USA PATRIOT Act, the Federal Bureau of Investigation (FBI) can access records held in the United States by applying for an order of the Foreign Intelligence Surveillance

> Act Court. A company subject to a section 215 order cannot reveal that the FBI has sought or obtained information from it. The risk of personal information being disclosed to government authorities is not a risk unique to U.S. organizations. In the national security and anti-terrorism context, Canadian organizations are subject to similar types of orders to disclose personal information held in Canada to Canadian authorities.[82]

The Commissioner ruled that the complaints were not well-founded, acknowledging that "many Canadians are concerned about the flow of their personal information outside of our country's borders and its accessibility by foreign governments. In order to determine whether these complaints are founded or not, however, it is the obligations imposed by the Act on Canadian-based organizations, and how well CIBC met them, that are the primary considerations."[83]

In reaching her determination, the Commissioner stated that "there is a comparable legal risk that the personal information of Canadians held by any organization and its service provider — be it Canadian or American — can be obtained by government agencies, whether through the provisions of U.S. law or Canadian law."[84] The comparable legal risk in both jurisdictions points to the relative weakness of both systems. Given the weak protections (as identified by the Supreme Court in *Spencer*), more robust reviews or accountability mechanisms within the Canadian surveillance framework may not address the foundational concern regarding the need for stronger privacy protections as part of any private sector disclosures of sensitive subscriber information.

Limited Privacy Protections Under US Law

Inadequate privacy laws are not limited to Canada. Indeed, ensuring adequate privacy protections for Canadians also requires pressuring our Five Eyes partners, particularly the United States, to grant universal privacy protections that apply equally to US and non-US persons. This is particularly true given the realities of the current cloud computing environment, where Canadians rely heavily on US-based services that store data in the United States and are subject to US law.

Unlike US persons, who enjoy legal protections through a variety of mechanisms aimed at respecting their constitutional privacy

rights and freedom of expression, non-US persons are granted limited protections through the definition of "foreign intelligence information." This includes information "with respect to a foreign power or foreign territory that relates to…the conduct of the foreign affairs of the United States."

Given this broad definition, non-US persons have practically no privacy protections. For example, the 2008 US *FISA Amendments Act* permits US authorities to seek broad certification to collect categories of foreign intelligence information for up to one year.[85] With such a certification in hand, authorities can then issue directives to US-based Internet companies such as Google or Facebook to compel them to disclose and decrypt information that falls within the broad terms of this certification. It should be noted certifications are not the equivalent of court orders and require a far lower evidentiary standard. Indeed, the US legislative approach grants authorities the power to engage in sweeping surveillance of both content and metadata of non-US persons whose data is stored within the United States.

This issue, which is canvassed more exhaustively in Lisa Austin's contribution in this volume,[86] suggests that the concerns for the Canadian privacy protections are not limited to the activities of Canadian security intelligence agencies and Canadian law. Indeed, with Canadian data regularly transiting across US communications networks, the absence of privacy protections for Canadians (i.e., non-US citizens) in the United States is a particular cause for concern. The issue is also one of the most difficult to address since improvements within domestic frameworks — whether on substantive provisions or oversight and accountability mechanisms — do not solve the lack of protection under US law. Indeed, the issue must be escalated between the countries, with Canadian officials seeking stronger protections in recognition of the increasingly integrated communications networks and surveillance agency activities.

Conclusion

As Canadians learn more about the current state of surveillance activities and technologies (including the ability to data mine massive amounts of information), there is a budding recognition that current surveillance and privacy laws were crafted for a much different world. The geographic or content limitations placed on surveillance

activities by organizations such as CSE may have been effective years ago when such activities were largely confined to specific locations and the computing power needed to mine metadata was not readily available.

That is clearly no longer the case. The law seeks to differentiate surveillance based on geography, but there is often no real difference with today's technology. Moreover, the value of metadata is sometimes greater than the actual content of telephone conversations. The current law provides few privacy protections and ineffective oversight in the face of intelligence agencies investing billions of dollars in surveillance technologies and telecommunications and Internet companies providing assistance that remains subject to court-imposed gag orders.

The legal framework leaves Canadians with twentieth-century protections in a world of twenty-first-century surveillance. The recent call for improved oversight and accountability of Canada's surveillance agencies is both understandable and long overdue. However, the bigger challenge will be to address the substantive shortcomings of the current Canadian legal framework as well as the limitations found in foreign frameworks that have a direct impact on the privacy of Canadians. Indeed, improved oversight without addressing the limitations within current law threatens to leave many of the core problems in place. For Canadians concerned with the privacy implications of seemingly ubiquitous surveillance and a legal framework that does not reflect current technologies or network practices, doing a better job of watching the watchers is not enough.

Acknowledgements

My thanks to several anonymous reviewers for their helpful comments on earlier versions of this chapter and to Emily Murray for her research and citation assistance. Any errors or omissions are the sole responsibility of the author.

Notes

1. Chris Strome & Margaret Talev, "Obama Unveiling NSA Changes in Response to Snowden Leaks," *Bloomberg News*, 17 January 2014, <http://www.bloomberg.com/news/articles/2014-01-17/obama-unveiling-nsa-changes-in-response-to-snowden-leaks>.

2. See, e.g., Randal Milch, "Verizon Releases Transparency Report for First Half 2014," 8 July 2014, *Verizon Policy Blog*, <publicpolicy.verizon.com/blog/entry/verizon-releases-transparency-report-for-first-half-2014>.
3. See, e.g., "Transparency Report," (2014) ATT, <about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html>.
4. Greg Weston, "Snowden Document Shows Canada Set up Spy Posts for NSA," *CBC News*, 9 December 2013, <www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886>.
5. David Patton, "Telus Issues First 'Transparency Report' on Requests for Customer Information," *Toronto Star*, 18 September 2014, <www.thestar.com/business/2014/09/18/telus_issues_first_transparency_report_on_requests_for_customer_information.html>.
6. Colin Freeze et al, "TekSavvy, Rogers Break Silence Over Government Requests for Data," *Globe and Mail*, 5 June 2014,<http://www.theglobeandmail.com/technology/tech-news/teksavvy-opens-books-on-government-data-requests/article18999107/>.
7. Canadian Press, "Disclosure of 'Sensitive' Telecom Surveillance Details Worried Feds: Memo," *Maclean's*, 30 November 2014, <www.macleans.ca/news/canada/disclosure-of-sensitive-telecom-surveillance-details-worried-feds-memo/>.
8. Bill C-13, *An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Sess, 41st Parl, 2015 (as passed by the House of Commons 20 October 2014) [Bill C-13].
9. Bill C-51, *An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, 2nd Sess., 41st Parl., 2015 (first reading 30 January 2015), [Bill C-51].
10. "NSA Leaks on Canadian Surveillance Coming, Greenwald Says," *CBC News*, 9 November 2013, <www.cbc.ca>.
11. On Canadian concerns with surveillance, see Colin J. Bennett et al, eds., *Transparent Lives: Surveillance in Canada* (Edmonton: Athabasca University Press, 2014).
12. "NDP Wants Parliamentary Oversight of Government's Intelligence and Security Activities," 29 October 2013, *New Democratic Party of Canada*, <www.ndp.ca/news/ndp-wants-parliamentary-oversight-governments-intelligence-and-security-activities>. See also Craig Forcese, "Faith-Based Accountability: Metadata and CSEC Review," 13 February 2014, *National Security Law* (blog), <craigforcese.squarespace.com/national-security-law-blog/2014/2/13/faith-based-accountability-metadata-and-csec-review.html>.

13. James Cox, "Canada and Five Eyes Intelligence Community," (2012) Canada International Council, Working paper, <www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf>. See also Colin Freeze, "'Five Eyes' Intelligence Sharing Program Threatens Canadians Abroad, Watchdog Warns," *Globe and Mail*, 31 October 2013, <http://www.theglobeandmail.com/news/politics/five-eyes-intelligence-sharing-program-threatens-canadians-abroad-watchdog-warns/article15199925/>.
14. See generally Kevin Walby & Seantel Anaïs, "Communications Security Establishment Canada (CSEC): Structures of Secrecy, and Ministerial Authorization after September 11," (2012) 27:3 *Canadian Journal of Law and Society* 363; Martin Rudner, "Canada's Communications Security Establishment from Cold War to Globalization," (2001) 16:1 *Intelligence and National Security* 97; Martin Rudner, "Canada's Communications Security Establishment, Signals Intelligence and Counter Terrorism," (2007) 22:4 *Intelligence and National Security* 473; and Stéphane Lefebvre, "Canada's Legal Framework for Intelligence," (2010) 23:2 *International Journal of Intelligence and Counterintelligence* 247.
15. *National Defence Act*, RSC 1985, c N-5, s. 273.64.
16. *Ibid*.
17. Canada, Office of the Communications Security Establishment Commissioner, *2011–2012 Annual Report* (Ottawa: Public Works and Government Services Canada, 2012).
18. *House of Commons Debates*, 41st Parl., 1st Sess., No. 266 (10 June 2013), (Hon. Andrew Scheer).
19. *Ibid*.
20. *Bill C-51*, *supra* note 9.
21. Canada, Office of the Communications Security Establishment Commissioner, *2012–2013 Annual Report* (Ottawa: Public Works and Government Services Canada, 2013).
22. Mitch Potter & Michelle Shephard, "Canada's Electronic Watchers Enjoy Secrecy Second to None," *Toronto Star*, 9 November 2013, <http://www.thestar.com/news/world/2013/11/09/canadas_electronic_watchers_enjoy_secrecy_second_to_none.html>.
23. See generally Roy Rempel, "Canada's Parliamentary Oversight of Security and Intelligence," (2004) 17:4 *International Journal of Intelligence and CounterIntelligence* 634.
24. Bill C-81, *An Act to establish the National Security Committee of Parliamentarians*, 1st Sess., 38th Parl., 2005 (first reading 25 November 2005).
25. Bill C-551, *An Act to establish the National Security Committee of Parliamentarians*, 2nd Sess., 41st Parl., 2013 (first reading 7 November 2013).
26. Bill C-622, *An Act to amend the National Defence Act (transparency and accountability, to enact the Intelligence and Security Committee of Parliament*

Act and to make consequential amendments to other Acts, 2nd Sess., 41st Parl., 2014 (first reading 18 June 2014).
27. National Information Standards Organization, "Understanding Metadata," (2004) *NISO Press*, <www.niso.org/publications/press/UnderstandingMetadata.pdf>.
28. "ST-09-9002 Working Draft: Office of the Inspector General," (24 March 2009), National Security Agency, Central Security Service, Working paper ST-09-0002, <www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf>.
29. Ryan Lizza, "The Metadata Program in Eleven Documents," *New Yorker*, 13 December 2013, <http://www.newyorker.com/news/daily-comment/the-metadata-program-in-eleven-documents>.
30. *Ibid*.
31. Stephane Couture & Catherine Pappas, "Surveillance and Metadata Collection in Canada," (2014) GISWatch, <giswatch.org/en/country-report/communications-surveillance/canada>.
32. Colin Freeze, "Data-Collection Program Got Green Light from MacKay in 2011," *Globe and Mail*, 10 June 2013, <http://www.theglobeandmail.com/news/politics/data-collection-program-got-green-light-from-mackay-in-2011/article12444909/>.
33. Senate of Canada, Proceedings of the Standing Committee on National Security and Defence, 1st Sess., 39th Parl., No. 15 (30 April 2007), online: <www.parl.gc.ca/Content/SEN/Committee/391/defe/15evb-e.htm?comm_id=76&Language=E&Parl=39&Ses=1>.).
34. Ron Deibert, "Spy Agencies Have Turned Our Digital Lives Inside Out. We Need to Watch Them," *Globe and Mail*, 10 June 2013, <http://www.theglobeandmail.com/globe-debate/spy-agencies-have-turned-our-digital-lives-inside-out-we-need-to-watch-them/article12455029/>.
35. Jay Stanley & Ben Wizner, "Why The Government Wants Your Metadata," *Reuters*, 7 June 2013, <http://blogs.reuters.com/great-debate/2013/06/06/why-the-government-wants-your-metadata/>.
36. Canada, Office of the Privacy Commissioner of Canada, *What an IP Address Can Reveal About You: A Report Prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada*, by Technology Analysis Branch, May 2013, <www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.asp>.
37. Ontario, Information and Privacy Commissioner, *A Primer on Metadata: Separating Fact from Fiction*, July 2013, <www.privacybydesign.ca/content/uploads/2013/07/Metadata.pdf>.
38. *R. v. Vu*, 2013 SCC 60 at para. 42, [2013] 3 SCR 657.
39. Bill Robinson, "Metadata and Second Parties," (2 December 2013, *Lux Ex Umbra* (blog), <www.luxexumbra.blogspot.ca/2013/12/metadata-and-second-parties.html>.

40. David Cole, "'We Kill People Based on Metadata,'" 10 May 2014, *New York Review of Books Blog*, <www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/>.
41. Alan Rusbrigder, "The Snowden Leaks and the Public," (2013) 60:18 *New York Review of Books*, <www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/>.
42. *American Civil Liberties Union v. United States (National Security Agency & Federal Bureau of Investigation, 959 F Supp (2d) 724 (SD NY 2013) lead to appeal to 2nd Cir granted*, (*Amici Curiae* Brief of Experts in Computer and Data Science in Support of Appellants and Reversal), *<www.eff.org/document/computer-scientists-amicus-aclu-v-clapper>.*
43. See generally Nicholas Koutros & Julien Demers, "Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement," (2013) 11 CJLT 79 (WL Can).
44. Section 20, *Bill C-13*, *supra* note 8.
45. *Ibid.*
46. Tonda MacCharles, "Tories Deny Canadian Spy Agencies Are Targeting Canadians," *Toronto Star*, 10 June 2013, <www.thestar.com/news/canada/2013/06/10/tories_deny_canadian_spy_agencies_are_targeting_canadians.html>.
47. "Frequently Asked Questions," 8 August 2014, *Communications Security Establishment*, <www.cse-cst.gc.ca/en/about-apropos/faq>.
48. Office of the Privacy Commissioner of Canada, "Outsourcing of canada.com E-mail Services to U.S.-Based Firm Raises Questions for Subscribers," Findings under the *Personal Information Protection and Electronic Documents Act* Case Summary #2008-394, <www.priv.gc.ca/cf-dc/2008/394_20080807_e.asp>.
49. Mitch Potter & Michele Shephard, "Canadians Not Safe From U.S. Online Surveillance, Expert Says," *Toronto Star*, 7 June 2013, <www.thestar.com/news/world/2013/06/07/canadians_not_safe_from_us_online_surveillance_expert_says.html>.
50. For an expert discussion on Canadian surveillance technologies and the likely activities of Research in Motion, see Ron Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: Signal, 2013).
51. Asad Ismi, "Massive Secret Surveillance in Canada," 1 November 2013, *The Monitor*, <https://www.policyalternatives.ca/publications/monitor>.
52. Section 2, *Bill C-51*, *supra* note 9.
53. *Ibid*., Schedule 3.
54. *Ibid*., s. 6.
55. Canada Border Services Agency, "North American Partnerships," 12 January 2007, *CBSA*, <www.cbsa-asfc.gc.ca/agency-agence/partner-partenaire-eng.html>.

56. Royal Canadian Mounted Police, "Integrated National Security Enforcement Teams," 18 July 2014, *RCMP*, <www.rcmp-grc.gc.ca/secur/insets-eisn-eng.htm>.
57. Canada's Economic Action Plan, "Perimeter Security & Economic Competitiveness," *Canada's EAP*, <actionplan.gc.ca/en/page/bbg-tpf/canada-us-border-cooperation>.
58. *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c. 17.
59. *Department of Citizenship and Immigration Act*, SC 1994, c. 31, s. 4.
60. *IN THE MATTER OF an application by [Redacted] for a warrant pursuant to Sections 12 and 21 of the Canadian Security Intelligence Service Act, RSC 1985, c C-23; AND IN THE MATTER OF [Redacted]*, 2013 FC 1275. <leaksource.files.wordpress.com/2013/12/mosley-csis.pdf>.
61. Craig Forcese, "Triple Vision Accountability and the Outsourcing of CSIS Intercepts," 6 December 2013, *National Security Law* (blog), <craigforcese.squarespace.com/national-security-law-blog/2013/12/6/triple-vision-accountability-and-the-outsourcing-of-csis-int.html>.
62. *Supra* note 21 at 19.
63. Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Acts*, 2nd Sess., 41st Parl., 2014, (first reading 27 October 2014) [Bill C-44].
64. *Canadian Security Intelligence Service Act* s. 8(2), being part of *Bill C-44*.
65. Craig Forcese, "Foreign Spying, Information Sharing & Arar Commission Fixes to Accountability: Brief on Bill C-44," 27 November 2014, *National Security Law* (blog), <craigforcese.squarespace.com/national-security-law-blog/2014/11/27/foreign-spying-information-sharing-arar-commission-fixes-to.html>. See also Canadian Civil Liberties Association, "Submission on Proposed Changes to CSIS Act (Bill C-44)," 26 November 2014, *CCLA*, <ccla.org/2014/11/26/cclas-submissions-on-proposed-changes-to-csis-act-bill-c-44/>.
66. European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, European Parliament, <www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0//EN> at 12/52.
67. *Ibid.*
68. Michael Geist, "Canada – European Union Data Sharing Agreement Sent to EU Court of Justice for Review," 3 December 2014, *Michael Geist* (blog), <www.michaelgeist.ca/2014/12/canada-european-union-data-sharing-agreement-sent-eu-court-justice-review/>.
69. *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5.

70. *Ibid.* at s. 26(2)(b).
71. *Ibid.* at s. 7(3)(c).
72. Michael Geist, "Canadian Telcos Asked to Disclose Subscriber Data Every 27 Seconds," 30 April 2014, *Michael Geist* (blog), <www.michaelgeist.ca/2014/04/telco-disclosures/>.
73. Colin Freeze, "Border Agency Asked for Canadians' Telecom Info 18, 849 Times in One Year," *Globe and Mail*, 27 March 2014, <http://www.theglobeandmail.com/news/politics/telecoms-routinely-give-customer-information-to-canada-border-service-agency/article17691103/>.
74. Michael Geist, "RCMP Records Called 'Incomplete and Inaccurate' in Memo," *Toronto Star*, 27 February 2015, <http://www.thestar.com/business/2015/02/27/rcmp-records-called-incomplete-and-inaccurate-in-memo-geist.html>.
75. Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, <https://www.ic.gc.ca/eic/site/icgc.nsf/vwapj/ETHI-e.pdf/$file/ETHI-e.pdf> at 6.
76. *R v Spencer*, 2014 SCC 43, 375 DLR (4th) 255.
77. *Ibid.* at para. 46.
78. *Ibid.* at para. 66.
79. *Ibid.* at para. 73.
80. *Supra* note 62 at s. 7(3)(c.1).
81. Office of the Privacy Commissioner of Canada, "Bank's Notification to Customers Triggers *PATRIOT Act* Concerns," Findings under the *Personal Information Protection and Electronic Documents Act* Case Summary #2005-313, <www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp>.
82. *Ibid.*
83. *Ibid.*
84. *Ibid.*
85. US, Bill HR, *Foreign Intelligence Services Act of 1978 Amendments Act of 2008*, 110th Cong, 2008, s. 702 (enacted).
86. See Austin, Chapter IV.

Page left blank intentionally