7

Systematic Government Access to Private-Sector Data in Canada

JANE BAILEY AND SARA SHAYAN

I. INTRODUCTION

In Canada, information privacy is implicitly constitutionally protected by the Charter of Rights and Freedoms (Charter), as well as by provincial, territorial, and federal privacy statutes that regulate the collection, use, retention, and disclosure of personal information.[1] The Privacy Act regulates federal government institutions' relationship with personal information,[2] whereas private sector organizations' relationship with personal information is regulated by the federal Personal Information and Protection of Electronic Documents Act (PIPEDA) or by any substantially similar legislation promulgated in the province in which the private entity operates.[3] These protections, however, are subject to numerous exceptions that allow, and even encourage, information sharing between government entities and between private-sector and state entities.

Statutes enabling law enforcement access to personal information generally require prior authorization, subject to numerous exceptions. Domestic law enforcement agencies obtain prior authorization under the Criminal Code (Code),[4] whereas Canada's primary national security intelligence gathering agencies—the Communications Security Establishment (CSE)[5] and the Canadian Security Intelligence Service (CSIS)—are subject to more relaxed provisions in their respective enabling statutes. National security concerns in relation to

1. Canadian Charter of Rights and Freedoms, being Part I of the Constitution Act 1982.

2. Privacy Act, RSC 1985, c. P-21.

3. Personal Information and Protection of Electronics Documents Act, SC 2000, c. 5.

4. Criminal Code of Canada, RSC 1985, c. C-46, as amended.

5. The Communications Security Establishment (CSE) is sometimes also referred to as the Communications Security Establishment of Canada (CSEC).

Bulk Collection. Fred H. Cate and James X. Dempsey.

large financial transactions and air travel have also led to laws requiring certain private-sector entities to gather and disclose personal information about their clients to government agencies. Canadian law enforcement agents' access to data outside of the jurisdiction generally arises from formal and informal networks, and from requests for assistance from partners under Mutual Legal Assistance Treaties (MLATs).

Although the CSE's capacity to intentionally surveil communications in Canada without ministerial authorization is limited, the agency continuously surveils foreign signals intelligence in cooperation with other signatories to the UK-USA Security Agreement (popularly known as the "Five Eyes"). The Snowden disclosures revealed substantial cooperation between the CSE and its international intelligence partners, with leaked documents showing that the CSE tracked travelers using wi-fi in a Canadian airport, participated in extensive surveillance operations in Brazil and Mexico, surveilled millions of Internet downloads, and helped to set up numerous international spy posts for the United States' National Security Agency.[6]

The Privacy Commissioner of Canada (PCC) and his or her provincial and territorial counterparts play an active role in informing Canadians about information privacy issues, including transborder flows of Canadians' personal information. All privacy commissioners have taken an active role in public debate relating to law enforcement demands for greater access to data and greater secrecy in investigation. The recently-passed Protecting Canadians from Online Crime Act (Bill C-13), Protection of Canada from Terrorists Act (Bill C-44), and Anti-Terrorism Act, 2015 (Bill C-51) have made it easier for state actors to obtain and share information about Canadians domestically and abroad, resulting in what the current PCC has called "a sea change for privacy rights in Canada."[7]

6. Greg Weston, Glenn Greenwald, and Ryan Gallagher, "CSEC Used Airport Wi-Fi to Track Canadian Travellers: Edward Snowden Documents," *CBC News* (January 30, 2014), http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881; Greg Weston, Glenn Greenwald, and Ryan Gallagher, "Snowden Document Shows Canada Set Up Spy Posts for NSA," *CBC News* (December 9, 2013), http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886; The Associated Press, "Canadian Spies Targeted Brazil's Mines Ministry: Report" (October 7, 2013), http://www.cbc.ca/news/canadian-spies-targeted-brazil-s-mines-ministry-report-1.1927975; Amber Hildebrandt, "CSE Spying in Mexico: Espionage Aimed at Friends 'Never Looks Good,'" *CBC News* (March 25, 2015), http://www.cbc.ca/news/canada/cse-spying-in-mexico-espionage-aimed-at-friends-never-looks-good-1.3005887; Amber Hildebrandt, Michael Pereira, and Dave Seglins, "CSE Tracks Millions of Downloads Daily: Snowden Documents," *CBC News* (January 27, 2015), http://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120.

7. Privacy Commissioner of Canada, *2014–2015 Privacy Act Annual Report to Parliament: Protecting Personal Information and Public Trust* (December 2015) at 15, https://www.priv.gc.ca/information/ar/201415/201415_pa_e.asp; see Protecting Canadians from Online Crime

Public debate surrounding the Snowden disclosures and controversial national security legislation enacted in subsequent years has highlighted the need for improved oversight and accountability mechanisms. The National Security and Intelligence Committee of Parliamentarians Act (Bill C-22) would, if enacted, address some of these concerns by creating a new committee of parliamentarians with the authority to review national security and intelligence issues across federal departments, subject to some exceptions.[8]

II. NATIONAL LEGAL CONTEXT AND FUNDAMENTAL PRINCIPLES

Canada is a parliamentary democracy founded on the rule of law. Canada's Constitution Act specifies the heads of power of the federal and provincial/territorial governments, whereas the Charter guarantees enumerated rights and freedoms applicable against all levels of government.[9] Any law inconsistent with the Constitution is of no force or effect. Information privacy has constitutional status in Canada, not through explicit Charter guarantees, but as a result of the interpretation of guarantees relating to the right against unreasonable search and seizure (s. 8) and, to a lesser extent, to life, liberty, and security of the person (s. 7).[10]

Provincial/territorial and federal privacy commissioners also play a role in the protection of personal information and data privacy, with oversight powers relating in some cases both to private sector and government operations. Although they tend to have only limited direct enforcement powers, privacy commissioners play an important role in raising public awareness about privacy rights and data security. The limited enforcement powers of the PCC is one issue that, at the time of writing, is under consideration by The House of Commons' Standing Committee on Access to Information, Privacy and Ethics as it conducts a review of PIPEDA.

Act, SC 2014, c. 31; Protection of Canada from Terrorists Act, SC 2015, c. 9; Anti-terrorism Act, 2015, SC 2015, c. 20.

8. Bill C-22, *An Act to establish the National Security and Intelligence Committee of Parliamentarians and to make consequential amendments to certain Acts,* 1st Sess, 42nd Parl, 2016 (passed by the House of Commons, April 4, 2017 and passed second reading and referred to committee by Senate on May 30, 2017).

9. The Constitution Act, 1982, being Sched. B. to the Canada Act 1982 (UK), c. 11.

10. Notable exceptions in which privacy has been examined outside the § 8 criminal context include § 7 challenges mounted against provincial laws relating to the confidentiality of sperm donor and adoption records: *Pratten v. BC (AG)* 2011 BCSC 656; *Cheskes v. Ontario (Attorney General)*, 2007 CanLII 38387 (ON SC).

III. CONSTITUTIONAL, STATUTORY, AND REGULATORY OVERVIEW

A. Constitutional Law

The Canadian Charter of Rights and Freedoms protects "reasonable" expectations of privacy, with reasonableness determined on a "normative rather than descriptive" standard.[11] As a result, the growth and prevalence of surveillance technologies should not *per se* diminish the objective reasonableness of an expectation of privacy.

Section 8 rights are only triggered in relation to information if an individual subjectively expected his or her information to be kept private, and if that subjective expectation was reasonable. The reasonableness of an expectation of privacy depends upon an analysis of the "totality of the circumstances" in which an alleged search or seizure takes place.[12] "Core biographical information" that reveals "intimate details" about a person's lifestyle and individual choices is one kind of information that definitely attracts a reasonable expectation of privacy.[13] Where a reasonable expectation of privacy is found to exist in relation to information, authorities generally cannot obtain that information without prior authorization. The Supreme Court of Canada (SCC) has recognized a reasonable expectation of privacy in, inter alia, personal computers; work-issued computers; cellular phones, regardless of whether they are password-protected; and Internet Service Provider (ISP) subscriber data, but no reasonable expectation of privacy in patterns of heat emanating from a home, or patterns of electricity use measured by a digital recording ammeter.[14] In 2016, a provincial court affirmed a reasonable expectation of privacy in cell phone records, and held that a "tower dump" production order implicating more than 30,000 mobile phone users was overly broad and clearly violated section 8.[15]

As emerging surveillance technologies increasingly permit collection of new types of information or bits of data that were previously inaccessible, Canadian courts have struggled with the question of whether the bits themselves must constitute "core biographical information" in order to trigger section 8 protection, or whether section 8 can be triggered where these bits may combine with other information to facilitate an inference about intimate lifestyle choices. Despite differences of opinion in lower courts, the SCC held in 2014 that Canadians have

11. *R. v. Tessling*, [2004] 3 SCR 432, at 42.

12. *R. v. M. (M.R.)*, [1998] 3 S.C.R. 393, at 286.

13. *R. v. Gomboc,* 2010 SCC, at 28.

14. *R. v. Morelli,* 2010 SCC 8, at 2–3 (personal computers); *R. v. Cole*, 2012 SCC 53, at 59 (work-related computers); *R. v. Fearon*, 2014 SCC 77, at 53 (cell phones); *R. v. Spencer*, 2014 SCC 43, at 66 (ISP subscriber data); *Tessling*, above note 11, at 63 (heat patterns); *Gomboc*, above note 13, at 1 (electricity usage).

15. *R. v. Rogers Communications*, 2016 ONSC 70.

a reasonable expectation of privacy in ISP subscriber information. Section 8 accordingly protects the "link between [an] identified individual and personal information provided anonymously," and extends to overlapping understandings of privacy as secrecy, control, and anonymity.[16]

Information held by a third party with no obligation to maintain confidentiality in relation to it may not be subject to a reasonable expectation of privacy. The SCC has concluded that, although not determinative, contractual waivers of confidentiality may be a factor in assessing the reasonableness of any claimed expectation of privacy in relation to data disclosed by private-sector entities to police.[17]

Searches and seizures without prior authorization may pass constitutional muster if a reasonable law permitted the search and the authorities conducted themselves reasonably.[18] For example, a cell phone search incident to a lawful arrest will not violate section 8 if the search is sufficiently tailored, and if police take detailed notes of what they searched and why.[19] Statutory provisions allowing for voluntary compliance with police requests for disclosure of particular data (such as the one in PIPEDA, discussed below) or mandatory reporting to state agencies (such as those relating to financing of terrorist organizations discussed below in Section III(D)) may also be constitutionally permissible without prior authorization, so long as they are properly tailored to minimize intrusions on privacy (e.g., to apply only in exigent circumstances and/or in circumstances where there are reasonable and probable grounds to believe an offense is being committed in the place to be searched). Bill C-13, which came into force in March 2015, amended the Criminal Code such that any person who voluntarily provides requested information to a public official without a warrant or production order will not incur any civil or criminal liability for doing so (s. 487.0195(2)).

Canadian courts tend to strain against indiscriminate surveillance premised on a "generalized suspicion" even in relation to public spaces and communications facilities (with notable exceptions in relation to airports, border crossings, and intelligence gathering for national security purposes).[20] Even in the context of terrorism investigations, courts have sought to protect the privacy interests

16. *Spencer*, above note 14, at 42, 38.

17. *Gomboc*, above note 13.

18. *R. v. Collins*, [1987] 1 SCR 265.

19. *Fearon*, above note 14.

20. *R. v. Thompson*, [1990] 2 SCR 1111 (public spaces and communications facilities); *R. v. AM,* [2008] 1 SCR 569 (border crossings); Ian Kerr, "Searching for the Right Balance", (May 1, 2008), *Ian Kerr* (blog) (border crossings), http://iankerr.ca/content/2008/05/05/searching-for-the-right-balance/; Re Canadian Security Intelligence Service Act, 2008 FC 301 (CanLII) (national security intelligence); *Re X*, [2010] 1 FCR 460 (national security intelligence).

of unrelated third parties by including minimization provisions in intercept authorization orders.[21]

B. Statutory Law

The privacy of personal information is also protected in federal and provincial/territorial legislation. Government collection, use, retention, and disclosure of personal information is regulated by applicable legislation in each province and territory, and through the Privacy Act at the federal level. For private sector organizations involved in commercial activity, the collection, use, retention, and disclosure of personal information is regulated by the federal PIPEDA, unless the organization is statutorily exempted or the organization operates in a province or territory with legislation declared substantially similar to the federal legislation.[22] In the latter case, the organization's information practices would be governed by the relevant, substantially similar provincial or territorial legislation.[23]

Both the Privacy Act and PIPEDA have been recognized as fundamental laws of Canada and therefore enjoy quasi-constitutional status on the basis that protection of privacy is an essential component of a democracy.[24] For similar reasons, although most privacy commissioners' authority is limited by comparison with their European counterparts, their reports and submissions play an important role in developments relating to the Canadian information privacy framework.

1. The *Privacy Act*—Regulation of Federal Government Institutions

The purposes of the Privacy Act, which came into effect in 1983, are twofold: (1) to protect personal information[25] held by federal government institutions,

21. *R. v. Ansari,* 2010 ONSC 1316, at 31–32.

22. Whether PIPEDA is ultra vires Parliament's powers under § 91 of the Constitution Act has been challenged, but not determined. *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada*, 2010 FC 736 (CanLII).

23. In this regard, British Columbia, Alberta, and Quebec have laws recognized as substantially similar to PIPEDA, and Ontario has enacted laws relating to health information that are also recognized as substantially similar. Canada has 10 provinces and 3 territories. Given space constraints and the fact that PIPEDA or statutes substantially similar to PIPEDA regulate privacy protection in private-sector entities, this chapter focuses on the federal legislation.

24. *Eastmond v. Canadian Pacific Railway*, 2004 FC 852; *Lavigne v. Canada (Office of the Commissioner of Official Languages),* 2002 SCC 53 (CanLII).

25. Personal information includes inter alia information relating to race, age, religion, marital status, education, address, and fingerprints relating to an individual; views or opinions of another about an individual; and the individual's name where it appears with other personal information relating to that individual: Privacy Act, § 3.

including the Royal Canadian Mounted Police (RCMP), CSIS, and CSE; and (2) to provide individuals with a right of access to their information (s. 2). The Privacy Act regulates federal government institutions' collection, use, retention, and disclosure of personal information as follows:

- *collection*—of personal information only if it "relates directly to an operating programme or activity of the institution" (s. 4) and generally is to be collected from the individual directly (s. 5(1));
- *retention*—for a period of time (that may be prescribed by regulation or set out in institutional policies) that would ensure the individual to whom it relates "has a reasonable opportunity to obtain access" to it (s. 6(1));
- *disposal*—in accordance with regulations, directives, or guidelines of the minister designated in relation to that federal institution (s. 6(3)), with "federal institutions [being] required to develop retention and disposal schedules to manage their records"[26] (although they do not always do so[27]);
- *use*—limited to the original purpose for obtaining the information, or a use consistent with that purpose, or a purpose for which the information was disclosed to the institution by another institution (s. 7); and
- *disclosure*—from one federal institution to another is prohibited, except for a long list of exceptions including disclosure to designated investigative bodies for purposes of enforcing Canadian or provincial laws or pursuant to arrangements or agreements with other institutions, governments of foreign states, etc. for purposes of administering or enforcing laws or carrying out investigations (s. 8(2)).

The PCC is appointed under the Privacy Act and is empowered to investigate complaints and make recommendations (ss. 34–35) as well as to periodically audit government handling of personal information (s. 37).

2. PIPEDA—Regulation of Private Sector Organizations

PIPEDA was enacted in 2000 for the stated purpose of promoting "electronic commerce by protecting personal information[28] that is collected, used or

26. Privacy Commissioner of Canada, *Privacy and Aviation Security: An Examination of the Air Transport Security Authority, Final Report* (2011), http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_catsa_2011_e.pdf.

27. Privacy Commissioner of Canada, *Audit of Selected RCMP Operational Databases Final Report* (2011), http://www.priv.gc.ca/information/pub/ar-vr/ar-vr_rcmp_2011_e.cfm. [hereinafter PCC *RCMP*].

28. Personal information "means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." PIPEDA, § 2.

disclosed in certain circumstances by providing for the use of electronic means to communicate or record information or transactions" (s. 3). PIPEDA applies to every organization in relation to personal information that it "collects, uses or discloses in the course of commercial activities" or is about an employee of a federal work, undertaking, or business. It expressly does not apply to any government institution governed by the Privacy Act (s. 4(2)). All organizations governed by PIPEDA must comply with a list of obligations set out in Schedule 1 of the Act, which sets out the Model Code for the Protection of Personal Information. The Model Code requires compliance with 10 fair information practices relating to accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, and individual access (Schedule 1). As noted above, at the time of writing, the House of Commons Standing Committee on Access to Information, Privacy and Ethics was holding hearings as part of its review of the data protection provisions of PIPEDA, which s. 29 of the Act requires to be conducted every five years. Eventually, this review could yield future amendments to the Act.

Generally, under PIPEDA, private sector organizations that handle personal information must obtain consent from individuals before collecting, using, or disclosing personal information, and must limit collection, use, and disclosure to predefined purposes. Personal information can only be retained as long as necessary to fulfill the purpose for which it was originally collected. However, these restrictions are subject to numerous exceptions. For example, consent to collection, use, and disclosure is not required where "inappropriate" because, inter alia, the information is being collected for law enforcement purposes and seeking consent might defeat the purposes of that investigation. Likewise, personal information may be used or disclosed for purposes other than its original purposes if required by law. Further, an individual's right to access information about the existence, use, and disclosure of personal information may be limited for legal or security reasons. These exceptions to the general fair information practice rules outlined in the Model Code are reflected in certain exceptions within the body of PIPEDA itself.

PIPEDA section 7 allows private sector organizations to collect, use, and disclose personal information about an individual without his or her knowledge or consent in a variety of circumstances (s. 7(1), 7(2), 7(3)), including for purposes relating to law enforcement. Although the frequency with which these exceptions are used is not consistently publicly reported, the most prominent provision publicly discussed is section 7(3), which allows private organizations to, inter alia, disclose personal information without knowledge or consent where disclosure is made to a government institution that has requested the information, identified its lawful authority to obtain the information, and indicated that it suspects the information relates to national security; enforcement of a Canadian, provincial, or foreign law; or is requested for purposes of administering a Canadian or provincial law. Private-sector organizations may also voluntarily collect personal information without notice or consent for similar kinds of purposes. Individuals' general rights relating to disclosure of how private

organizations are dealing with their personal information under PIPEDA are also subject to exceptions, including with respect to disclosures made under section 7(3). In these situations, the government must be notified of the request and may effectively veto disclosure to the individual of even the fact that the individual's personal information was disclosed to government (ss. 8 and 9).

The PCC is empowered to investigate individual complaints lodged under PIPEDA and to issue reports and recommendations for corrective action in relation to them (ss. 12 and 13). Although the recommendations themselves are not legally enforceable, courts can be called upon to review the PCC's decisions and to issue orders. The PCC may also conduct audits and promote the purposes of the *Act* through information programs and public research, and is empowered to share information with other commissioners (s. 24).[29]

C. Specific Laws for Law Enforcement Access, Regulatory Access, and/or National Security Access

1. Basic Organizational Concepts and the Antiterrorism File

In 2003, the federal government created a department focused on issues relating to national security, which since 2006 has been called Public Safety Canada (PSC). PSC reports to the Minister of Public Safety (MPS) and was created to "ensure coordination across all federal departments and agencies responsible for national security and the safety of Canadians."[30] In February 2012, the MPS unveiled Canada's first comprehensive counterterrorism strategy, setting as its first priority to "counter domestic and international terrorism in order to protect Canada, Canadians, and Canadian interests."[31] One component of the strategy is to detect terrorists, terrorist organizations, and their supporters through investigation, intelligence operations, and analysis, which the PSC notes will require "extensive collaboration and information sharing with domestic and international partners."[32]

The strategy identifies three primary federal government intelligence collection organizations: CSIS, the CSE, and the RCMP. Other federal agencies, including the Department of National Defence (DND), the Department of Foreign Affairs and International Trade, the Canada Border Services Agency (CBSA), Transport Canada, and the Financial Transactions and Reports Analysis Centre (FINTRAC) are also to be involved in information collection "in support of

29. Provincial and territorial privacy commissioners also have investigatory, audit, and educative functions in relation to violations of their respective pieces of legislation. Virtually all, however, have noted that a lack of resources undermines their capacity in these areas.

30. Public Safety Canada, *About Public Safety Canada* (November 27, 2015), http://www.publicsafety.gc.ca/cnt/bt/index-eng.aspx.

31. Public Safety Canada, *Building Resilience against Terrorism: Canada's Counter-Terrorism Strategy* (2011), http://www.publicsafety.gc.ca/prg/ns/_fl/2012-cts-eng.pdf.

32. Ibid.

their primary responsibilities," which assist with developing "a broader counter-terrorism intelligence picture."[33] A key priority of the strategy appears to be ensuring information exchange between and amongst these domestic players, as well as with similar agencies acting for international partners. Since the 2015 enactment of Bill C-51, over a hundred government departments are authorized to share information for national security purposes, facilitating investigation into "activities that undermine the security of Canada."[34]

2. Domestic Law Enforcement and the General Requirement for Prior Authorization

Canada has federal, provincial, and municipal law enforcement agencies. The RCMP is the federal law enforcement agency, and is also intimately involved in the terrorism file. Domestic law enforcement agencies' search and seizure powers are generally constrained by the need for prior judicial authorization, subject to exceptions such as those outlined below.

Under Code section 184, willful interception of "private communication"[35] is a crime, except in specific circumstances. For example, the general prohibition on interception does not apply to, inter alia, interceptions with prior judicial authorization (s. 184(2)), or non-pre-authorized interceptions made by a peace officer in certain urgent situations involving imminent unlawful acts that there are reasonable grounds to believe "would cause serious harm to any person or property" (s. 184.4). Generally, prior authorization is only to be granted where a number of criteria are met, including that alternative methods of investigation have been tried and failed, or are unlikely to succeed, or are impractical because of urgency (s. 185). However, the alternative methods criteria is not required to be satisfied for offenses involving a criminal organization or terrorism (s. 185(1.1)). Judicial authorizations must be specific with regard to the type of private communication intercepted, and must include any other terms necessary to protect the public interest (s. 186(4)). Targets of interception must generally be notified within 90 days of the order, although there are provisions that allow for extensions of this time period, particularly in relation to terrorism offenses.

Following passage of Bill C-13, a judge issuing an interception order can also issue "a search warrant, a general warrant, make a general production order, make a specific production order to obtain certain information (such as computer data

33. Ibid.

34. Security of Canada Information Sharing Act, SC 2015, c. 20, § 2, § 5(1).

35. A "private communication" is "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it." Code, § 183.

or financial information), make an assistance order or issue a warrant to use a tracking device or a 'transmission data recorder.'"[36] As a result, law enforcement agencies are now authorized to make a demand or obtain a court order to preserve electronic evidence if they have reasonable grounds to *suspect*, among other things, that an offense under Canadian or foreign law has been committed (s. 487.012) and courts can make ex parte preservation and production orders to trace a specified communication, to obtain transmission data, to obtain tracking data, and to obtain financial data when requested on similar grounds (s. 487.013; 487.015; 487.016; 487.017; 487.018). Judges issuing these kinds of preservation and production orders are also authorized to issue orders prohibiting disclosure of their existence or content in certain circumstances (s. 487.0191). Judges may also issue warrants to obtain transmission data in real time and to permit remote activation of tracking devices in certain types of technologies (s. 492.1; 492.2).[37] Finally, although C-13 amendments state that preservation demands, preservation orders, and production orders are not necessary in order for law enforcement officers to ask a person to preserve or produce a document (s. 487.0195), this provision must be read in light of the *Spencer* decision, which requires prior authorization.

One area that had been controversial is whether certain forms of digital communications ought to be treated as "private communication" and therefore subject to the prior authorization regime for interception rather than the regular warrant provisions relating to searches of persons, places, or things. The regular warrant provisions are arguably easier to satisfy than the intercept authorization provisions, as the former do not require the issuing justice to be satisfied that there are no reasonable alternative investigative methods (s. 487).[38] In 2013, the SCC held that law enforcement officials must obtain prior authorization under the interception regime before accessing text messages held by telecommunications providers, noting that text messages are private communications, and that "[t]echnical differences inherent in new technology should not determine the scope of protection afforded to private communications."[39] The SCC also recently held that law enforcement officials must obtain a separate warrant before searching the contents of a computer (although officers may, under the general warrant regime, seize a computer and take measures to preserve its data until a separate search warrant is issued).[40]

36. Julia Nicol & Dominique Valiquet, *Legislative Summary of 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* (Dec. 11, 2013), http://www.lop.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=C13&Parl=41&Ses=2#a27.

37. Ibid.

38. Craig Forcese, *National Security Law: Canadian Practice in International Perspective* (2008), at 451.

39. *R. v. Telus Communications,* 2013 SCC 16, at 5.

40. *R. v. Vu*, 2013 SCC 60.

Under section 195 of the *Code*, the MPS must produce an annual report on electronic surveillance in Canada, describing, inter alia, the number of pre-authorization applications made and granted, the average time for which authorizations are issued, the types of offenses investigated using electronic surveillance, and the general methods of interception used. In 2015, PSC reported 67 applications for authorization (44 pursuant to ss. 185, 22 pursuant to section 487.01, and 1 renewal pursuant to s. 186), all of which were granted.[41]

3. Intelligence Agencies

Under PSC's counterterrorism strategy, three agencies are primarily tasked with intelligence gathering functions relating to national security: CSE, CSIS, and the RCMP.

CSE is housed under the DND, which is responsible for Canadian military operations. Under provisions added to the National Defence Act (NDA) with the passage of the Anti-terrorism Act in 2001, CSE is authorized to: (1) collect foreign signals intelligence, (2) assist with protection of Canada's information infrastructures, and (3) provide technical and operational assistance to federal law enforcement and security agencies.[42] However, section 273.64(2)(a) of the NDA limits CSE's mandates under (1) and (2) by prohibiting it from directing its activities at Canadian citizens, permanent residents, or corporations wherever they are, or at anyone in Canada regardless of nationality. Where one-end Canadian communications are unintentionally intercepted, CSE is only permitted to retain them if it is "essential to either international affairs, defence or security, or to identify, isolate or prevent harm to Government computer systems or networks."[43]

However, the Minister of National Defence (MND) may authorize CSE to intercept private communications if satisfied that certain criteria are met (e.g., where interception is necessary to CSE's foreign intelligence mandate) (s. 273.65 *NDA*). As a result, unlike domestic law enforcement agencies, CSE need not seek prior *judicial* authorization to intercept private communication of Canadians, and the ministerial authorizations it obtains last longer than intercept authorizations under the Code and need never be disclosed to those whose communications were intercepted. Although a former CSE Commissioner opined that the ministerial authorization process is Charter compliant, others argue that judicial oversight is necessary (while recognizing that this weaker form of authorization may be found justifiable under the Charter on the basis of "national security").[44]

41. Public Safety Canada, *2015 Annual Report on the Use of Electronic Surveillance*, at 5 (2015), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2015/lctrnc-srvllnc-2015-en.pdf.

42. Communications Security Establishment Commissioner, *Annual Report 2010–2011*, at 3, https://www.ocsec-bccst.gc.ca/s21/s46/s16/eng/2010-2011-annual-report.

43. Ibid., at 4.

44. Forcese, above note 38, at 456–58.

In performing its mandate (3), CSE's powers are limited in the same ways as those of the agencies it is assisting.[45] CSE's operations are subject to review by the CSE Commissioner.

CSE gathers foreign intelligence through its participation in the SIGINT network operated by Australia, Canada, New Zealand, the UK, and the United States as signatories to the UK-USA Security Agreement. The network, which is popularly referred to as Echelon or "Five Eyes," is reportedly capable of intercepting, inter alia, phone calls and data traffic globally (including emails) through various networks, including the telephone network.[46] Documents leaked by Edward Snowden confirm and expand upon these reports, describing CSE metadata collection programs and extensive assistance afforded to Five Eyes partners.[47]

CSIS, which lies within the authority of the MPS, was created with passage of the *CSIS Act* in 1984 and is mandated to aid in the protection of national security. In pursuit of its mandate, CSIS collects, analyzes, and retains intelligence relating to activities it has reasonable grounds to suspect threaten the security of Canada, and reports and advises the Canadian government with respect to that intelligence. Its powers are limited to collecting only that which is "strictly necessary" to its mandate, and it must only undertake investigations with "demonstrable grounds for suspicion" of a threat to national security.[48] CSIS's operations are subject to review by the Security Intelligence Review Committee (SIRC).

CSIS has its own warrant provisions under the CSIS Act, which allow it to obtain prior judicial authorization for searches relating to threats to the security of Canada or to permit it to assist the MND or Minister of Foreign Affairs to gather intelligence relating to the capability, intention, or activity of foreign actors. These authorization provisions (which have withstood constitutional scrutiny)[49] allow for orders entitling CSIS to search or seize a variety of materials and places and to "install, maintain or remove any thing" (in relation to interception activities). They may last up to 60 days and never require notification of the target after the search has been completed. Bill C-44, the Protection of Canada from Terrorists Act, amended the CSIS Act in 2015 to explicitly authorize CSIS to perform its duties within or outside Canada (CSIS Act §§ 12(2), 15(2)).

45. CSEC, *Annual Report 2010–2011*, above note 42, at 8.

46. Gerhard Schmid, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON interception system)* (European Parliament: Temporary Committee on the ECHELON Interception System, July 11, 2001), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN.

47. Michael Geist, "Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (2014) 225–55.

48. Forcese, above note 38, at 84, 457–58.

49. Ibid., at 452.

Further, the Federal Court is now authorized to issue warrants allowing CSIS to conduct activities both within and outside of Canada in order to investigate threats to national security regardless of "any other law, including that of a foreign state" (CSIS Act § 21(3.1)).

The RCMP, in addition to its role as Canada's national police force, is specifically vested with exclusive authority to police national-security related crimes. As a result, despite the creation of CSIS in 1984, the RCMP continues to be involved in intelligence collection relating to crimes involving a "threat to the security of Canada" (which is defined in the CSIS Act).[50]

As intelligence gathering is increasingly centralized through Integrated Security Units (ISUs) for particular events such as the Olympics and G8 meetings, the national security functions of the RCMP and other Canadian police forces have become increasingly intermeshed with those of CSIS. The centralization of antiterror and national security intelligence functions in Canada through ISUs and the Integrated Threat Assessment Centre formed by CSIS in 2007 has been compared to US fusion centers.[51] Others have suggested a need to formally increase the integration of CSE, the RCMP, and FINTRAC in order to better protect critical infrastructure against terrorist attack.[52]

Review of Canada-wide RCMP activities (ranging from "officer rudeness to allegations of the use of unnecessary force") is conducted by the Civilian Review and Complaints Commission for the RCMP.[53] Although the RCMP's national security investigations and investigatory powers have expanded in recent years, there has not been a commensurate increase in resources granted to the Commission. Furthermore, despite strict secrecy legislation, the Commission may be denied access to secret information where the RCMP cites a need to protect operational information and foreign intelligence sources.[54]

4. Regulatory Agencies

Numerous regulatory agencies at the federal and provincial/territorial level are empowered to require disclosure from private sector entities in relation to their mandates. This chapter addresses only the two federal agencies that seem most pertinent: the Canadian Radio-television and Telecommunications Commission (CRTC) and the Competition Bureau.

50. Ibid. at 88.

51. Jeffrey Monaghan & Kevin Walby, "Making up 'Terror Identities': Security Intelligence, Canada's Integrated Threat Assessment Centre and Social Movement Suppression" (2011) *Policing and Society* 1, 3–4.

52. Kosta Rimsa, "Eavesdroppers" in Dwight Hamilton, ed, *Inside Canadian Intelligence*, at 141–42 (2011).

53. Craig Forcese & Kent Roach, *False Security: The Radicalization of Canadian Anti-terrorism*, at 434 (Irwin Law, 2015).

54. Ibid., at 434–35.

The CRTC regulates broadcasting[55] and telecommunications[56] in Canada pursuant to, respectively, the Broadcasting Act (BA) and the Telecommunications Act (TA).[57] The CRTC has largely chosen to forebear from regulating retail mobile and Internet services (including billing, rates, service quality, or ISP business practices) because it has concluded there is sufficient competition in these areas.[58] It has also largely exempted from regulating new media broadcasting undertakings (NMBU) that deliver broadcasting[59] services over the Internet and via P2P technology received over mobile devices.[60] NMBUs are, however, subject to an undue preference prohibition.[61] However, the CRTC does regulate certain aspects of wholesale Internet services, and handles complaints about Internet traffic management practices at both the retail and wholesale level.[62] Complaints about other ISP practices are directed to the Commissioner for Complaints for Telecom Services,[63] whereas complaints regarding Internet content are directed to the Canadian Association of Internet Service Providers for examination under its Code of Conduct or to the appropriate law enforcement agency where illegal content is in issue.[64] The CRTC does, however, monitor and report on broadcasting, telecommunications, and Internet-related developments annually, using survey data obtained

55. " '[B]roadcasting' means any transmission of programmes, whether or not encrypted, by radio waves or other means of telecommunication for reception by the public by means of broadcasting receiving apparatus, but does not include any such transmission of programmes that is made solely for performance or display in a public place." BA, § 2(1).

56. " '[T]elecommunications' means the emission, transmission or reception of intelligence by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system." *TA*, § 2(1).

57. Broadcasting Act, SC 1991, c. 11, as amended; Telecommunications Act, SC 1993, c. 38, as amended.

58. CRTC, *Internet—Our Role* (June 28, 2016), http://www.crtc.gc.ca/eng/internet/role.htm.

59. Conflicting opinions around whether ISPs qualify as broadcasters under the *BA* and concerns around the ways in which convergence is rendering obsolete distinctions such as telecom and broadcasting have led, respectively, to a CRTC commitment to refer the broadcaster question to the Federal Court and a CRTC call for development of a national digital strategy. CRTC, *Broadcasting Regulatory Policy, CRTC 2009-329* (June 4, 2009)

60. CRTC, *Public Notice CRTC 1999-197* (December 17, 1999), http://www.crtc.gc.ca/eng/archive/1999/pb99-197.htm; CRTC, *Broadcasting Regulatory Policy, CRTC 2009-329* (June 4, 2009).

61. CRTC, *Broadcasting Regulatory Policy*, above note 60.

62. CRTC, *Internet—Our Role*, above note 58.

63. CRTC, *How to Make a Complaint about Your Internet Service* (May 27, 2015), http://www.crtc.gc.ca/eng/internet/plaint.htm.

64. CRTC, *TV and Music Online* (April 2, 2014), http://crtc.gc.ca/eng/internet/musi.htm#internet.

from industry providers.[65] The Telecommunications Act and Broadcasting Act empower the CRTC to issue policies, implement licensing regimes, compel licensees to submit information relating to their operations, and (in relation to hearings it is empowered to hold) compel production and inspection of documents and entry and inspection of property (Broadcasting Act, ss. 9, 10, 16; Telecommunications Act, ss. 55, 58, 67).

In recent years, the CRTC has begun exercising its authority to issue search warrants, in some cases carrying out investigations "in close collaboration with its partners, including the Federal Bureau of Investigation, Europol, Interpol, Microsoft Inc., the Royal Canadian Mounted Police (RCMP), Public Safety Canada and the Canadian Cyber Incident Response Centre."[66] The CRTC successfully carried out a warrant to enter a building associated with an antivirus telemarketing scam in November 2015,[67] and used powers conferred under Canadian anti-spam legislation to take down a command and control server hosting malware one month later.[68]

The Competition Bureau (Bureau) is an independent law enforcement agency responsible for administering and enforcing, inter alia, the Competition Act, including in relation to telecommunications undertakings.[69] It has a variety of powers to compel disclosure of information and its own statutory process to obtain warrants to authorize searches and seizures connected with its mandate domestically. It can also obtain warrants to assist international agencies involved in competition-related matters in respect of which the Mutual Legal Assistance in Criminal Matters Act (MLACMA) applies.[70] The Bureau has also worked closely with domestic law enforcement agencies, such as the RCMP, in relation to mass marketing fraud (including online), as well as identity theft.

D. Laws Requiring Broad Reporting of Personal Data by Private Sector Entities

1. National-Security Related Provisions

A number of federal laws require private-sector entities to report personal data to governmental agencies or statutorily created regulatory bodies, often in relation

65. CRTC, *CRTC Communications Monitoring Report* (2011), http://www.crtc.gc.ca/eng/publications/reports/PolicyMonitoring/2011/cmr2.htm#n0.

66. CRTC, "CRTC Serves Its First-Ever Warrant under CASL in Botnet Takedown" (December 3, 2015), http://news.gc.ca/web/article-en.do?nid=1023419.

67. CRTC, "CRTC Executes First Inspection Warrant as Part of Telemarketing Investigation" (November 27, 2015), http://news.gc.ca/web/article-en.do?nid=1022319.

68. CRTC, "CRTC Serves Its First-Ever Warrant under CASL in Botnet Takedown," above note 66.

69. Competition Act, RSC 1985, c. C-34.

70. Mutual Legal Assistance in Criminal Matters Act, RSC 1985, c. 30 (4th supp.).

to matters of public or national security. Since 2000, in what the PCC characterized as "precedent setting" legislation, certain private-sector entities have been mandated to collect and disclose information to a government agency, without prior authorization for or demonstration of reasonable grounds to compel these acts.[71] The Proceeds of Crime (Money Laundering) and Terrorist Financing Act requires a wide variety of government agencies, individuals, and business entities engaged in what might broadly be described as financial services (e.g., banks, loan and trust companies, casinos, foreign exchange services) to keep and retain records relating to prescribed transactions (e.g., "large cash" transactions in excess of $10,000) and to report these transactions within a specified time period to FINTRAC.[72]

The reports include a variety of personal information, including the name, address, telephone number, and personal identifier of an individual who has conducted a large cash transaction.[73] All of these entities are also required to report to FINTRAC "every financial transaction that occurs or that is attempted in the course of their activities" where there are reasonable grounds to suspect that the transaction related to commission or attempted commission of a money laundering or "terrorist activity financing offence."[74]

Although FINTRAC is at arm's length from law enforcement agencies, it may disclose information it has received to law enforcement officials where it has "reasonable grounds to suspect" the information would be relevant to investigating or prosecuting money laundering or terrorism offenses or a threat to Canadian security.[75] Similarly, financial institutions are required to determine on a continuing basis whether they are "in possession or control of property owned or controlled by or on behalf of" an entity listed in the Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism and to report to

71. Privacy Commissioner of Canada, *Submission to the Standing Committee on Banking, Trade and Commerce re: Bill C-25, An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and the Income Tax Act and to make a consequential amendment to another Act* (December 31, 2006), http://www.priv.gc.ca/parl/2006/sub_061213_e.cfm.

72. Proceeds of Crime (Money Laundering) and Terrorist Financing Act, § 2000, c. 17.

73. FINTRAC, *Guideline 7A: Submitting Large Cash Transaction Reports to FINTRAC Electronically* (December 2016), http://www.fintrac-canafe.gc.ca/publications/guide/guide7A/lctr-eng.asp.

74. "Terrorist activity financing offences" include providing or collecting property for terrorist activities (including offenses implementing various international conventions related to acts such as hostage taking, unlawful acts of violence in airports, terrorist bombings), providing or making available property or services for terrorist purposes, and using or possessing property for terrorist purposes. Code, §§ 83.01, 83.02, 83.03, 83.04.

75. Senate Canada, *Security Freedom and the Complex Terrorist Threat: Positive Steps Ahead, Interim Report of the Special Senate Committee on Anti-terrorism*, at 36 (March 2011), http://www.parl.gc.ca/Content/SEN/Committee/403/anti/rep/rep03mar11-e.pdf.

their respective regulators monthly either that they are or are not in possession or control of such property (*Code* § 83.11).

Concerns relating to terrorism and threats to national security have also led to compelled disclosure of passenger and travel data from commercial carriers under the Passenger Protect Program (which was expanded after the Secure Air Travel Act came into effect following passage of Bill C-51). CBSA operates an advance passenger information (API) and passenger name record (PNR) program pursuant to which it requires commercial airlines to provide it with basic data relating to travelers' names, dates of birth, gender, citizenship, travel document, type of ticket, travel date, and related flight information prior to their arrival in Canada.[76] The CBSA also collects a "limited set" of the PNR data collected by air carriers or their agents relating to all passengers seeking entry into Canada, which includes "basic identity data," contact, payment, and billing information about their booking agent, as well as the traveler's check-in status, seating, and baggage information.[77] CBSA can use PNR to "to identify persons who have or may have committed a terrorism offence or a serious transnational crime [e.g. narcotics smuggling, human trafficking]" or to develop trend analysis or risk indicators for identifying people who have or may commit such offenses or crimes.[78] CBSA maintains API and PNR data in an access-restricted database (PAXIS) for a maximum of six years after receipt (CBSA, Guidelines). CBSA is authorized to disclose PNR to domestic authorities including CSIS, as well as to federal, provincial, and municipal police forces on a case-by-case basis subject to certain conditions. It can also disclose PNR to a foreign government authority on a case-by-case basis, so long as there is an international agreement in place to provide for that disclosure (CBSA, Guidelines). Records of disclosure must be kept and individuals have rights to request access to, request correction of, and to complain to the PCC about the PNR the CBSA holds about them (CBSA, Guidelines).

The MPS maintains a list of people he or she has reasonable grounds to believe will, among other things, threaten transportation security or use air travel to commit a terrorism offense—commonly referred to as the no-fly list.[79] The MPS can direct an air carrier, among other things, not to allow persons on the list to travel by air or require them to screen listed persons.[80] The Ministers of Transport and of Citizenship, the RCMP, CSIS, CBSA, and other persons authorized by regulation can assist the MPS in collecting and disclosing information

76. Canada Border Services Agency, *Guidelines for the Access to, Use, and Disclosure of Advance Passenger Information (API) and Passenger Name Record (PNR) Data, Memorandum D-1-16-3* (May 31, 2016), http://www.cbsa-asfc.gc.ca/publications/dm-md/d1/d1-16-3-eng.html; Secure Air Travel Act, SC 2015, c. 20, § 11, § 5(2).

77. CBSA *Guidelines*, above note 76.

78. Ibid.

79. Secure Air Travel Act, above note 76, § 8(1)

80. Ibid., § 9(1).

and the MPS can also enter into agreements with foreign states to disclose all or part of the list to them.[81] Individuals whose names appear on the list and have been denied travel can apply to the MPS to have their names removed, however, notwithstanding a report in November 2016 that a federal system of redress was under consideration, as of the date of writing no such system was as yet available.[82] Various prohibitions in the Secure Air Travel Act limit the bodies that have access to the list from disclosing it for purposes other than those provided for in the Act.[83]

The Immigration and Refugee Protection Act also authorizes certain officials to request disclosure of passenger information from commercial carriers.[84]

2. Other Kinds of Provisions

A variety of provincial legislation also compels disclosure of personal information, including with respect to public health. For example, the Ontario Health Protection and Promotion Act requires health care practitioners to report to the local public health authority the name, address, date of birth, health card number, gender and telephone number of any person infected or suspected of being infected with a listed communicable disease.[85]

E. Laws Permitting or Restricting Private Sector Entities from Providing Government Officials with Voluntary Broad Access to Data

Privacy laws in various provinces and territories[86] (as well as certain other kinds of legislation[87]) allow private-sector entities to share personal information with government officials in certain situations. Of these, the PIPEDA section 7

81. Ibid., §§ 10, 12.

82. Ibid., § 15(1); Michelle Zilio, "Ottawa Tight-Lipped on Delay to Improving No-Fly List" (April 10, 2017) *The Globe and Mail* http://www.theglobeandmail.com/news/politics/ottawa-tight-lipped-on-delay-to-improving-seriously-deficient-no-fly-list-database/article34662667/.

83. Ibid., §§ 20–21.

84. Forcese, above note 38, at 472.

85. Health Protection and Promotion Act, RSO 1990, c. H.7, § 25.

86. The kinds of situations in which provincial and territorial privacy statutes permit private-sector entities to provide information to public officials includes those where disclosure is required or permitted by law, to minimize imminent health or safety risks, for research or statistical purposes, or "in the public interest." M. Lacroix et al., *The Reporting and Management of Personal Information and Personal Health Information to Control and Combat Infectious Disease: An Analysis of the Canadian Statutory and Regulatory Framework* (March 2004), http://www.phac-aspc.gc.ca/php- psp/pdf/privacy_analysis.pdf.

87. See, for example, § 10(3) of the Code of Conduct Regulation (Alta Reg 160/2003) enacted pursuant to Alberta's Electric Utilities Act, SA 2003, c. E-5.1, which explicitly permits hydro

provisions (discussed above in Section III(B)2) that allow for collection, use, and disclosure for purposes relating to law enforcement have tended to be the most prominent. Media reports, case law, and transparency reports produced by Canadian telecommunications providers suggest that many section 7(3) requests for disclosure seek subscriber information in relation to online child sexual exploitation investigations. Since the *Spencer* ruling in 2014, these requests must be made pursuant to a production order. Examples drawn from case law in which police have relied upon "PIPEDA requests" in order to access subscriber identity indicate that a standard form letter is used, in which the officer identifies that the officer is acting in his or her capacity as a law enforcement officer investigating a child sexual exploitation offense, requests disclosure of the last known customer name and address of the account associated with a specified IP address being used at a specified date and time, and identifies the legislative source from which the officer's authority to make the request derives (typically the constating act and/or regulations for the police force to which that particular officer belongs).

In its 2015 Transparency Report, Rogers Communications indicated that it complied with 83,871 requests for disclosure by law enforcement agencies, or 97 percent of requests made that year.[88] Telus Communications similarly received 57,167 requests in 2015,[89] while Canada's largest telecommunications provider, Bell, has yet to release any transparency reports.[90] Prior to the SCC's *Spencer* ruling in 2014, state access to ISP subscriber data required only five minutes of paperwork, with documents released through access to information requests suggesting that some telecommunications providers may have created law enforcement databases to make subscriber data readily accessible to state officials.[91]

providers to disclose personal information about their customers to a peace officer for the purpose of investigating an offense, unless disclosure is contrary to an express request by the customer. In *Gomboc*, a majority of the SCC concluded that the defendant's failure to specify that he wished his information to be kept confidential when granted the option to do so, made it possible for the hydro authority to voluntarily disclose that information to the police. However, the Court left to another day the question of whether the regulation itself was constitutional. Similar kinds of provisions may well be buried in any number of legislative or regulatory instruments at the federal, provincial, and territorial level.

88. Rogers Communications, *2015 Rogers Transparency Report* (May 2016), http://about.rogers.com/about/helping-our-customers/transparency-report.

89. Telus Communications, *Sustainability Report 2015, "Business Operations: Transparency*," https://sustainability.telus.com/en/business-operations/transparency-report/.

90. Michael Geist, "Why Telecom Transparency Reporting in Canada Still Falls Short," *Michael Geist* (blog) (May 30, 2016), http://www.michaelgeist.ca/2016/05/why-telecom-transparency-reporting-in-canada-still-falls-short/.

91. Jim Bronskill, "RCMP Drops Some Internet-Related Probes Following Supreme Court Ruling," *CBC News* (November 21, 2014), http://www.cbc.ca/news/politics/rcmp-drops-some-internet-related-probes-following-supreme-court-ruling-1.2844390; Michael Geist, "The Spencer Effect: No More Warrantless Access to Subscriber Info with Five Minutes of

Apart from PIPEDA requests, it is clear that law enforcement and intelligence agencies interact with and rely upon private sources of information in a variety of ways, including through data mining techniques that scan publicly available information online,[92] as well as through purchasing information from private-sector data brokers.[93] However, the exact nature, extent, and prevalence of these practices remains unclear.

F. Role of the Courts

The courts play a central role in delineating the parameters within which the government may gain access to personal information in various capacities discussed above, including: articulating the constitutional parameters surrounding access, reviewing and (where applicable) enforcing decisions by privacy commissioners, and hearing and deciding applications for warrants and prior judicial authorizations for interceptions. In 2013, Federal Court Justice Richard Mosley held that that CSIS breached its duty of candor when it solicited help from Five Eyes partners while executing a surveillance warrant.[94] Furthermore, as noted above, the 2014 SCC ruling on voluntary disclosure of subscriber data in *Spencer* has had significant impact on Canadian private-sector disclosure norms, requiring that law enforcement seek pre-authorization before requesting subscriber data from ISPs.

G. Standards for Use, Access, Retention, and/or Destruction by Government

Standards for government use, access to, retention, and/or destruction of information about individuals are set first and foremost by the Privacy Act for federal institutions and by various provincial and territorial privacy acts for their respective jurisdictions. The key provisions in the federal legislation are set out in detail in Section III(B)1 above. The sharing of information among the CSE, CSIS, and the RCMP through memorandums of understanding technically permitted under the Privacy Act have been the subject of some controversy.

Police Work," *Michael Geist* (blog) (November 21, 2014), http://www.michaelgeist.ca/2014/11/spencer-effect-warrantless-access-subscriber-info-five-minutes-police-work/; Geist, Why Watching the Watchers, above note 47, at 243.

92. Security Intelligence Review Committee, *Checks and Balances: Viewing Security Intelligence Through the Lens of Accountability, Annual Report 2010–2011*, http://www.sirc-csars.gc.ca/pdfs/ar_2010-2011-eng.pdf.

93. Canadian Internet Policy and Public Interest Clinic, *On the Data Trail: How Detailed Information about You Gets into the Hands of Organizations with Whom You Have No Relationship, A Report on the Canadian Data Brokerage Industry* (April 2006), http://www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf.

94. *Re X,* 2013 FC 1275.

Of particular concern has been the possibility that the more onerous warrant provisions applicable to the RCMP might be circumvented through cooperation with CSIS and/or CSE, each of which has access to its own specific authorization provisions discussed above.[95] The more general issue of information sharing between law enforcement and intelligence agencies, and between Canadian agencies and foreign counterparts (particularly those who engage in torture) has also been canvassed in several prominent public inquiries.[96] Despite cautions against increased information sharing, Bill C-51 introduced provisions authorizing federal agencies and departments to share information pursuant to national security investigations, as discussed in more detail above.

H. Cross-Border and Multi-jurisdictional Issues

Participation in numerous information sharing arrangements and networks[97] to some degree facilitates law enforcement agencies' access to general information outside of Canadian borders through counterparts in other jurisdictions. More formal requests for access to such data can also be made from law enforcement officials in other countries under the numerous mutual legal assistance treaties to which Canada is a signatory.[98] Canada also cooperates with its co-signatories to the UK-USA Security Agreement, as noted above in Section III(C)3. Further, as discussed above, passage of Bill C-51 brought with it explicit authorization for sharing of certain kinds of information (such as no-fly lists) with foreign states.

Protecting the privacy of Canadians' data has certainly involved cross-border issues, particularly in relation to that data's accessibility to US authorities under the *PATRIOT Act*. For example, Canadian entities' outsourcing of data-related services to US entities generated recommendations from the British Columbia

95. CSEC, *Annual Report 2010–2011*, above note 42; Forcese, above note 38, at 501–02.

96. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/AR_English.pdf; Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy* (2010), http://publications.gc.ca/collections/collection_2010/bcp-pco/CP32-89-4-2010-eng.pdf; Frank Iacobucci, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almaki, Ahmad Abou-Elmaati and Muayyed Nureddin Final Report* (2008).

97. See, for example: the Virtual Global Taskforce Combatting Online Child Sexual Abuse, involving organizations from Canada, the United States, Australia, Europe and elsewhere: RCMP, *Virtual Global Taskforce: International Law Enforcement Working Together to Protect Children*, http://www.rcmp-grc.gc.ca/ncecc-cncee/vgt-eng.htm.

98. Included amongst the countries with whom Canada has signed such treaties are Australia, China, France, India, the United States, and numerous others. Information Exchange Network for Mutual Assistance in Criminal Matters and Extradition, *Principles Providing a Framework for Mutual Legal Assistance and Extradition and More Information: Canada 2004*, http://www.oas.org/juridico/mla/en/can/en_can-mla-gen-g8iag.html.

Privacy Commissioner in 2004 for, inter alia, legislation making it an offense to outsource the handling of a British Columbian's personal information outside of Canada.[99] A complaint to the PCC relating to the transborder flow of Canadians' personal information to a US data broker resulted in a judicial decision declaring that the PCC had jurisdiction to investigate the complaint, even though PIPEDA did not have extraterritorial effect.[100] Given that the PCC may assert jurisdiction in cases involving extraterritorial elements, so long as there is a real and substantial connection to Canada, the PCC has issued recommendations relating to Canadian companies' outsourcing of data-related services to firms in foreign countries, reminding Canadian entities of their PIPEDA obligations relating to notice and consent.[101] More recently, the PCC issued a publication identifying the privacy implications relating to cloud computing and reiterating the jurisdictional constraints and capacities of the Office of the Privacy Commissioner of Canada in relation to it.[102]

IV. RECENT CONTROVERSIES

The last five years have seen significant changes to Canadian national security and lawful access regimes, as well as dramatic revelations of bulk, indiscriminate, and pervasive international surveillance affecting and involving Canadians. Systematic domestic and international access to Canadian private-sector data remains a complex issue, governed by a patchwork of laws that feature many moving parts. As Lisa Austin notes, increased information sharing and the increasingly blurred investigatory roles of law enforcement, border control, and intelligence agencies have made "gaining a clear public understanding of proposed changes to lawful access laws or the full significance of legal cases before the courts [. . .] extremely difficult."[103] Although an extended discussion of the systemic effects of recent Canadian legislative changes lies beyond the scope of this chapter, we highlight some pertinent events, concerns, and controversies below.

In 2013, following the high-profile suicides of two Canadian teens, the Canadian government passed legislation prohibiting the non-consensual

99. Office of the Information and Privacy Commissioner for British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (October 2004), https://www.oipc.bc.ca/special-reports/1271.

100. *Lawson v. Accusearch Inc.*, 2007 FC 125.

101. *Outsourcing of Canada.com Email Services to US-Based Firms Raises Questions for Subscribers,* 2008 CanLII 58164 (PC).

102. Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues Related to Cloud Computing* (2010), http://www.priv.gc.ca/information/pub/cc_201003_e.cfm.

103. Lisa M. Austin, "Lawful Illegality: What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State," in Michael Geist, ed., *Law, Privacy, and Surveillance in Canada in the Post-Snowden Era* (2014) 103, 106.

distribution of intimate images, which also contained lawful access provisions long sought by Canada's previous federal government. Bill C-13 established new warrants and production orders for transmission, tracking, and financial data held by private-sector organizations, available to public officers who have reasonable grounds to suspect that an offense has been or will be committed under domestic law or under a law of a foreign state. As the current PCC notes, Bill C-13 leaves the definition of "public officers" broad, potentially offering "not just police, but anyone from a township reeve to a fisheries officer to a mayor with lawful access to personal information under reduced thresholds."[104] The new law also includes an immunity provision that "increases the likelihood of voluntary disclosures at the very time that Canadians are increasingly concerned with such activity,"[105] and imposes no good faith or reasonableness requirement on organizations that voluntarily disclose information to authorities. Others have further argued that the reasonable suspicion standard for metadata warrants in Bill C-13 seems at odds with the values underpinning the SCC's *Spencer* decision, which recognized a significant privacy interest in subscriber data held by ISPs.[106]

These changes take on new significance when considered alongside Bill C-51, a piece of controversial antiterror legislation passed in 2015. In addition to authorizing information sharing across federal departments for national security purposes, Bill C-51 makes changes to the no-fly list regime, and introduces provisions that criminalize knowingly advocating or promoting the commission of terrorism offenses in general. The new speech crime provisions in C-51 expand the range of situations where Bill C-13's metadata warrants may be issued, and raise the troubling possibility that "to detect the wrong type of speech, police may need to monitor all sorts of other speech during which the bad things might be said."[107] Furthermore, Bill C-51's permissive information sharing provisions may afford CSIS and other agencies indirect access to metadata that has been collected by police under the relaxed reasonable suspicion standard established in Bill C-13.[108]

Metadata collection in particular has become a matter of heightened public concern and debate in Canada in light of the 2013 Snowden revelations. The legal basis for CSE's metadata collection programs is the subject of an ongoing constitutional challenge by the British Columbia Civil Liberties Association and related "Stop Illegal Spying" public outreach campaign.[109] Furthermore, in

104. PCC, *2014–2015 Privacy Act Annual Report*, above note 7, at 14.

105. Michael Geist, *Testimony before the Justice and Human Rights Committee* (May 29, 2014), https://openparliament.ca/committees/justice/41-2/27/dr-michael-geist-1/only/.

106. John Geddes, "Cyberbulling, the Supreme Court and the Future of Bill C-13," *Maclean's* (June 21, 2014), http://www.macleans.ca/news/canada/suspicion-may-not-cut-it/.

107. Forcese & Roach, above note 53, at 127.

108. Ibid., at 128.

109. British Columbia Civil Liberties Association, "Stop Illegal Spying" (last visited April 26, 2017), https://bccla.org/stop-illegal-spying/.

light of recent insights into the extent of international spying, some have called for efforts to build more Canadian Internet exchange points, promote greater Canadian network sovereignty, and take measures to prevent data flow to countries with questionable privacy and surveillance practices.[110]

Despite having review bodies that can separately evaluate RCMP, CSE, and CSIS conduct, Canada currently lacks a body that can review cross-departmental national security activities. As Roach and Forcese write, "accountability bodies [in Canada] are restricted in the extent to which they can carefully scrutinise security service operations—each review body is 'siloed' to its own agency and cannot share confidential information."[111] Furthermore, as four former Canadian prime ministers noted in an open letter published during the debates surrounding Bill C-51, "the lack of a robust and integrated accountability regime for Canada's national security agencies makes it difficult to meaningfully assess the efficacy and legality of Canada's national security activities."[112]

In April 2017, the House of Commons approved Bill C-22, the National Security and Intelligence Committee of Parliamentarians Act and on May 30, 2017 the Senate referred the Act to Committee. If enacted, this bill would create a committee of parliamentarians with the power to review any matter or activity relating to national security or intelligence. Although public response to Bill C-22 has been largely positive to date,[113] some doubts remain as to whether the body will be able to act free of executive interference, and whether enhanced review can be effective without further substantive changes to the complex legal framework governing lawful access, information sharing, and national security investigations in Canada.[114]

110. Andrew Clement & Johnathan A. Ober, "Canadian Internet 'Boomerang' Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (2014) 13, 35.

111. Forcese & Roach, above note 53, at 145.

112. Jean Chrétien, Joe Clark, Paul Martin & John Turner, "A Close Eye on Security Makes Canadians Safer," *The Globe and Mail* (February 19, 2015), http://www.theglobeandmail.com/opinion/a-close-eye-on-security-makes-canadians-safer/article23069152/; Forcese & Roach, above note 53, at 400.

113. Ian McLeod, "Liberal Plan for New National Security Watchdog Gets Thumbs Up from Experts, Despite 'Inevitable Flaws,'" *National Post* (June 19, 2016), http://news.nationalpost.com/news/canada/canadian-politics/liberal-plan-for-new-national-security-watchdog-gets-thumbs-up-from-experts-despite-inevitable-flaws; Canadian Civil Liberties Association, "Bill C-22: A Step towards Real Accountability" (June 20, 2016), https://ccla.org/bill-c-22-a-step-towards-real-accountability.

114. Geist, Watching, above note 47, at 226; Austin, above note 103, at 104.

V. CONCLUDING OBSERVATIONS

Canada is at something of a crossroads in terms of expanded systematic state access to data held by the private sector. Constitutional and statutory norms protecting reasonable expectations of privacy from state intrusion generally underline the importance of prior judicial authorization and investigations focused by reasonable grounds relating to identifiable offenses. However, these norms have already been challenged by provisions that empower CSE to surveil Canadians' data with ministerial approval, compel private-sector organizations to collect and disclose personal information to authorities, and facilitate easier access to intercept authorization, if not warrantless access to data. Exceptions in the *Privacy Act* and PIPEDA that permit sharing of personal information between government institutions as well as recent provisions authorizing voluntary personal information disclosure by the private sector to law enforcement agencies further erode the standard of prior judicial authorization (subject to the SCC's findings in *Spencer*). Recent legislation authorizing information sharing among law enforcement, security agencies, other government officials, and, in some cases, foreign states, raises further cause for concern and presents challenges for meaningful and robust public accountability and oversight. Whether a newly proposed oversight committee would adequately address those challenges remains the subject of some controversy.