Government of Canada | Gouvernement du Canada

THIRD UPDATE REPORT ON

DEVELOPMENTS IN DATA PROTECTION LAW IN CANADA

Report to the European Commission June 2018

Canada

This publication is available online at http://www.ic.gc.ca/eic/site/113.nsf/eng/h_07662.html.

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/Publication-Request or contact:

Web Services Centre

Innovation, Science and Economic Development Canada

C.D. Howe Building

235 Queen Street

Ottawa, ON K1A 0H5

Canada

Telephone (toll-free in Canada): 1-800-328-6189

Telephone (international): 613-954-5031

TTY (for hearing impaired): 1-866-694-8389

Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)

Email: ISED@canada.ca

Cat. No. Iu37-8/3-2018E-PDF

ISBN 978-0-660-27388-4

Aussi offert en français sous le titre *Troisième rapport d'étape sur les évolutions en matière de législation sur la protection des données au Canada*.

Table of Contents

1. 0 Introduction

1.1 In December 2001, the European Commission (EC) issued Decision 2002/2/EC, pursuant to Article 25(6) of Directive 95/46/EC. The Decision states that Canada is considered as providing an adequate level of protection of personal data transferred from the European Union (EU) to recipients subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The adequacy decision was reaffirmed in 2006.

1.2 In accordance with Article 2 of Implementing Decision (EU) 2016/2295, which amended Decision 2002/2/EC, the EC is now required, on an ongoing basis, to monitor developments in the Canadian legal framework, including developments concerning access to personal data by public authorities, with a view to assessing whether Canada continues to ensure an adequate level of protection of personal data.

1.3 In May 2017, as part of an ongoing effort to assist the Commission in its monitoring obligation, Government of Canada officials provided EC officials with the first of several periodic reports outlining developments in Canada's data protection framework applicable to private sector organizations and government entities since Decision 2002/2/EC, as well as information on the limitations and safeguards governing the access to personal data by public authorities. An addendum report was subsequently provided to the Commission in September 2017 in response to a request for additional information.

1.4 In November 2017, Canada provided a second update report on privacy and data protection developments. Further engagement took place between Canadian and EC officials in a videoconference on February 16, 2018.

The present report:

- outlines developments in Canada's data protection framework since the second update report prepared in November 2017, and
- provides further information in Annex A, on items of interest raised by EC officials during the videoconference on February 16, 2018.

2.0 Developments Related to Canada's Private Sector Privacy Law

Breach of Security Safeguards Regulations under PIPEDA

2.1 On September 2, 2017, a regulatory proposal, titled *Breach of Security Safeguards Regulations*, was published for public consultation in the *Canada Gazette Part 1*. The proposal was made pursuant to statutory amendments for mandatory data breach reporting provided for under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in 2015. The objective of the Regulations is to provide greater certainty and specificity with respect to certain elements of the Act's data breach reporting requirements under Division 1.1.

2.2 The Government received approximately 20 written submissions from business associations, civil society, academics, experts in privacy law and data security, as well as the Office of the Privacy Commissioner (OPC). Stakeholders expressed general support for the proposed approach, which employs regulations to provide further details on statutory requirements for reporting breaches to the

Privacy Commissioner of Canada, for notification to affected individuals, and for record-keeping. The comments informed the development of the final regulations.

2.3 On April 18, 2018, the Government of Canada published the final Breach of Security Safeguards Regulations[1]. The Regulations will come into force on November 1, 2018. The Regulations set out how Canadian businesses are to alert individuals if their personal information is lost or stolen as a result of a data security breach and how they can protect themselves and their information. This includes specific requirements regarding the content, form and manner of reporting data breaches to the Office of the Privacy Commissioner of Canada as well as notification to affected individuals. The Regulations also stipulate a 24-month record-keeping requirement that extends to every breach of security safeguards of an organization. Financial penalties associated with failure to report a breach are outlined in the Regulations.

3.0 Legislative Initiatives

Bill C-49, Transportation Modernization Act, 2017

3.1 In May 2017, the Canadian government introduced legislation to amend the *Canada Transportation Act* and other Acts respecting transportation under Bill C-49, the *Transportation Modernization Act*[2]. The Bill addresses marine, air and rail transportation including amendments to the *Railway Safety Act* to require the installation of voice and video recorders in locomotive cabs to further enhance the safety of the rail transportation system in Canada. Bill C-49 received Royal Assent on May 23, 2018, making the installation and use of locomotive voice and video recorders mandatory to ensure that information is available for accident investigations while protecting the privacy of employees by limiting the purposes for which the data is used.

Bill C-76, Elections Modernization Act, 2018

3.2 On April 30, 2018, the Canadian government introduced legislation to amend the *Canada Elections Act* and other Acts and to make certain consequential amendments under the *Elections Modernization Act*[3]. The Bill addresses specific elements of Canada's electoral and political systems in the digital age including the collection of data by political parties. For example, the proposed legislation would require all political parties to create and publish a policy outlining how they will protect the privacy of voters, including what information they are collecting from potential voters, how it will be safeguarded and how it will be used. Second reading of the Bill, and referral to Committee in the House of Commons was completed on May 23, 2018. More details on the progress of this Bill will be provided in upcoming reports.

[1] The text of the Regulations, and the associated Regulatory Impact Analysis Statement, as published in the Canada Gazette Part II on Wednesday, April 18, 2018 (SOR/2018-64 on page 701) are available at http://gazette.gc.ca/rp-pr/p2/2018/2018-04-18/pdf/g2-15208.pdf
[2] Further information on Bill C-49, *the Transportation Modernization Act*, is available at https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=8945674&View=0
[3] Further information on Bill C-76, the *Elections Modernization Act*, is available at https://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=9808070

Bill C-59, National Security Act, 2017

3.3 The Canadian government has introduced legislation under Bill C-59, the *National Security Act*[4] that enhances the government's oversight of national security agencies and proposes amendments to the *Canadian Security Intelligence Service* (CSIS) *Act*. The Bill has been studied by the House of Commons Standing Committee on National Security and was reported back to the House of Commons, with amendments, on May 3, 2018. More recently, on June 11, the Bill was concurred in with amendments and will proceed to second reading.

3.4 Bill C-59 proposes that the National Security and Intelligence Review Agency (NSIRA) would replace the Security Intelligence Review Committee (SIRC). The NSIRA will be mandated to review public complaints regarding the conduct of CSIS, the Communications Security Establishment (CSE), the national security activities of the RCMP, and the denial or revocation of security clearances by the Government of Canada. The Government of Canada will have no say in what the NSIRA does or does not review, nor will it influence the findings of NSIRA reviews. In conducting reviews, the NSIRA will have full access to all government information, with the exception of Cabinet documents. NSIRA members will be expected to apply their independent judgement as citizens when making determinations regarding the appropriateness of government activities; they are not required to apply a pre-determined definition.

3.5 In terms of its composition, the proposed NSIRA will be led by up to seven members. These will be eminent Canadians – often with distinguished careers in parliament, public service or law – who will bring a diversity of backgrounds and experiences to bear on the work of the NSIRA. The NSIRA members will be supported by an expert secretariat.

3.6 The proposed NSIRA's complaints process will function much like that of its predecessor agency, SIRC. One or more NSIRA members will preside over quasi-judicial hearings. After the hearings are complete, the NSIRA will issue a report containing findings and recommendations.

3.7 Bill C-59 sets out the proposed oversight functions and responsibilities of the NSIRA as well as the National Security and Intelligence Committee of Parliamentarians (NSICOP)[5].The NSIRA and the NSICOP are both mandated to review the full range of national security and intelligence activities undertaken by the Government of Canada. While there is some potential for overlap, both bodies are legally required to coordinate their work to avoid unnecessary duplication. In practice, the NSICOP is expected to focus largely on high-level systemic issues, while the NSIRA will perform more detailed scrutiny of the legality of government operations. The two bodies will thus complement each other to ensure comprehensive scrutiny of government activities.

3.8 The Intelligence Commissioner, an oversight body, will be mandated to review the reasonableness of ministerial decisions regarding the use of certain powers by CSIS and CSE. In essence, CSIS or CSE will propose a certain action to the appropriate Minister. Once the Minister approves, the

[4] Further information on Bill C-59, the *National Security Act* is available at http://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=9057418

[5] The NSICOP was established under Bill C-22, *National Security and Intelligence Committee of Parliamentarians Act* which received Royal Assent in June 2017

Intelligence Commissioner will receive the same information that was provided to the Minister and have the opportunity to consider the reasonableness of the Minister's decision. If the Intelligence Commissioner does not find the decision to have been reasonable, then CSIS and CSE cannot take the action in question. The NSIRA and the NSICOP will follow up to ensure that these activities have been undertaken appropriately.

3.9 The Intelligence Commissioner process will supplement, but will not replace, the section 21 warrant regime. The Intelligence Commissioner will provide a new and additional layer of accountability for certain types of CSIS activities, notably activities for which a warrant is not required or would not be appropriate, but for which independent oversight is nonetheless important.

3.10 Bill C-59 also amends the CSIS Act to create a regime for CSIS to collect, retain, query and utilize datasets[6] in the course of performing its duties and functions, make amendments to the warrant regime that are related to datasets, and implement measures for the management of datasets. The proposed legislation applies to datasets which contain personal information as defined in the *Privacy Act.*

3.11 The proposed framework would include authorization by the Federal Court, or the new Intelligence Commissioner, for datasets which contain personal information that is not publicly available, and require a review by NSIRA, including the authority for NSIRA to refer its findings to the Federal Court as necessary. There would also be additional safeguards regarding the management of datasets, including segregating datasets containing non-publicly available personal information from CSIS' other investigative holdings, as well as strict controls on who can access them, requirements for record keeping, and for dataset retention and destruction.

3.12 The proposed legislation would also introduce a robust authorization regime for foreign datasets containing personal information predominately related to non-Canadians outside of Canada. Authorization from the Intelligence Commissioner would be needed for the retention of foreign datasets and, in exigent circumstances, the querying of Canadian or foreign datasets before their retention is authorized.[7]

4.0 Parliamentary Committee Activities

Statutory Review of Canada's Anti-Spam Legislation (CASL)

4.1 On December 13, 2017, the Standing Committee on Industry, Science and Technology (INDU) presented its report on the review of Canada's Anti-Spam Legislation. The report, titled Canada's Anti-Spam Legislation: Clarifications are in Order, makes 13 recommendations including clarification of certain legislative provisions of CASL and increasing education and transparency related to the Act.

[6] Bill C-59 defines a dataset as "a collection of information stored as an electronic record and characterized by a common subject matter".
[7] Further information is available at https://www.canada.ca/en/security-intelligence-service/news/2017/06/amendments_to_thecsisact-dataanalytics.html and https://www.canada.ca/en/services/defence/nationalsecurity/our-security-our-rights/questions-answers-strengthening-security-protecting-rights.html

4.2 The statutory review of CASL took place between September 26 and December 12, 2017. Throughout that period, the Committee held 13 meetings, heard from 41 witnesses and received 29 briefs from a wide array of stakeholders and experts.

4.3 The Government Response to the INDU Report on CASL was tabled before Parliament on April 16, 2018. The Response agrees wholly or in principle with all of the Report's recommendations and proposes to consult further with stakeholders on how to provide greater clarity to the Act, while maintaining its principles and inherent flexibility. The Response also notes that the Government agrees to work to improve coherence in education and guidance efforts while respecting the independence of enforcement agencies. It also agrees to investigate further the impact of implementing the private right of action and domestic information sharing with law enforcement agencies.

4.4 The Canadian Radio-television and Telecommunications Commission (CRTC) announced that it has entered into a Memorandum of Cooperation with Japan's Ministry of Internal Affairs and Communications to combat unsolicited commercial electronic messages. Under this Agreement, both jurisdictions agree to share information on a confidential basis, and provide investigative support to combat unwanted emails received by Canadian and Japanese residents. The Agreement builds on existing co-operation and sharing agreements the CRTC has concluded with some of Canada's international partners, including the United States, the United Kingdom, New Zealand and Australia. The Agreement[8], signed on December 8th, 2017, will support a coordinated approach in the enforcement of spam laws in both jurisdictions.

Study of the Personal Information Protection and Electronic Documents Act (PIPEDA)

4.5 On February 28, 2018, the Standing Committee on Access to Information, Privacy and Ethics (ETHI) issued its report on the study[9] of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The report, titled Towards Privacy by Design: Review of the *Personal Information Protection and Electronic Documents Act*, makes 19 recommendations covering all aspects of the Act, 13 of which propose legislative amendments. The recommendations generally fall under one of the following categories:

- Consent under PIPEDA;
- Online reputation;
- Enforcement powers of the Privacy Commissioner; and
- Impact of the EU General Data Protection Regulation.

4.6 Through the course of its study ETHI held a total of 16 public meetings during which 65 witnesses appeared from businesses, academia and privacy advocacy organizations. Of note were two appearances by the Privacy Commissioner of Canada, Mr. Daniel Therrien, who outlined a de facto scope for the study, and the appearance of the European Data Protection Supervisor, Mr. Giovanni Buttarelli, who provided testimony on the EU's General Data Protection Regulation (GDPR).

[8] The Memorandum of Cooperation is available at https://crtc.gc.ca/eng/internet/jpn.htm
[9] This work was a parliamentary study by the Committee as opposed to a statutory review of the legislation.

4.7 The Government Response to the ETHI report on PIPEDA was tabled before Parliament on June 19, 2018. The Response shares the Committee's view that changes are required to Canada's privacy regime and indicates the next step will be to engage Canadians on data and digital issues to explore how Canada can lead and succeed in a data and digitally-driven economy while at the same time protecting privacy. On the same day, the government launched national public consultations on digital and data transformation in order to better understand how Canada can drive innovation, prepare Canadians for the future of work and ensure they have trust and confidence in how their data is used. The National Digital and Data Consultations include national online public consultations and a series of roundtable discussions in cities across Canada with industry stakeholders, indigenous peoples and women.

Study of Breach of Personal Information Involving Cambridge Analytica and Facebook

4.8 On March 22, 2018, the Standing Committee on Access to Information, Privacy and Ethics (ETHI) adopted a motion to conduct a study of the privacy implications of platform monopolies and possible national and international regulatory and legislative remedies to assure the privacy of citizens' data and the integrity of democratic and electoral processes across the globe. On June 19, 2018, ETHI issued an interim report on its study of the breach of personal information involving Cambridge Analytica and Facebook. The report, titled Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process, summarizes the evidence the Committee has heard in the first months of its study and provides eight preliminary recommendations for consideration. These preliminary recommendations include proposals for the broader privacy framework (which echo the Committee's recommendations from its recent study of PIPEDA), as well as measures aimed specifically at protecting the integrity of Canada's democratic processes. ETHI intends to continue its study making additional recommendations in its final report once the study is completed.

5.0 Recent Court Decisions

Supreme Court of Canada

5.1 On December 8, 2017, the Supreme Court of Canada issued its decisions in *R. v. Marakah* and *R. v. Jones*, which dealt with the privacy rights of an accused's electronic communications. In these cases, the Supreme Court reaffirmed that, whether a claimant has a reasonable expectation of privacy must be answered with regard to the totality of the circumstances of a particular case. As part of its analysis, the court stated that a number of factors may assist in determining whether it was objectively reasonable to expect privacy in different circumstances, including: (1) the place where the search occurred; (2) the private nature of the subject matter, that is whether the informational content of the electronic conversation revealed details of the claimant's lifestyle or information of a biographic nature; and (3) control over the subject matter. As for control, the court found that it is not an absolute indicator of a reasonable expectation of privacy, nor is lack of control fatal to a privacy interest. As such, it is only one factor to be considered in the totality of the circumstances. In both decisions, the Supreme Court found that the individual had a reasonable expectation of privacy in the text messages they had sent even though the messages were no longer in their exclusive control.

6.0 OPC Guidance

Draft position on online reputation ("right to be forgotten")

6.1 In January 2018, the OPC published its Draft OPC Position on Online Reputation.[10] The draft document highlights existing protections in Canada's federal private sector privacy law, identifies potential legislative changes, and proposes other solutions for consideration. These measures include the right to ask search engines to de-index web pages that contain inaccurate, incomplete or outdated information; removal or amendment of information at the source; and education to help develop responsible, informed online citizens.

Guidelines for obtaining meaningful consent

6.2 On May 24, 2018, the OPC published Guidelines for obtaining meaningful consent.[11] The Guidelines set out seven guiding principles for meaningful consent under PIPEDA. The Office will begin to apply these guidelines on January 1, 2019.

6.3 On May 24, 2018, the OPC published Guidelines on the interpretation and application of section 5(3) of PIPEDA[12], essentially identifying "no-go zones" for the collection and use of personal information. Subsection 5(3) is a guiding principle that underpins the interpretation of the various provisions of PIPEDA. The OPC will begin to apply these guidelines on July 1, 2018.

7.0 Other Items of Interest

Artificial Intelligence

7.1 In June of 2017, the *Budget Implementation Act*, 2017 received Royal Assent authorizing funding of up to CAN$125,000,000 to the Canadian Institute for Advanced Research to support a pan-Canadian artificial intelligence strategy.[13] The objective of the strategy is to help strengthen Canada's leadership position in the area of artificial intelligence and establish an ecosystem of research and talent development.

7.2 In March 2018, the Treasury Board of Canada released an initial draft of its Standard on Automated Decision Making for public consultation. The proposed intent of the Standard is to allow the federal government to use automated decision-making systems to provide insights and recommendations on administrative decisions while ensuring that the data and systems that perform these functions are designed and operate responsibly and in compliance with Canadian and international law, standards, codes, rules and regulations. Once the Standard is final, it is expected that further non-binding guidance, in the form of a subsidiary Guideline, will be published to assist federal government institutions in complying with the Standard.

[10] The document is available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/
[11] The Guidelines are available at https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/
[12] The Guidelines are available at https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/
[13] See clause 115 of Bill C-44 available at http://www.parl.ca/DocumentViewer/en/42-1/bill/C-44/royal-assent

7.3 In the context of its 2018 G7 Presidency, Canada has advanced work internationally on artificial intelligence. In March 2018, Innovation Ministers expressed a shared vision of human-centric artificial intelligence for innovation and economic growth, and released a statement that confirms the need to safeguard privacy. This vision was also expressed by Leaders in their Common Vision Statement on Artificial Intelligence, and the G7 Leaders' Statement released in June 2018. Going forward, a multi-stakeholder conference on artificial intelligence will be hosted by Canada in the fall of 2018. This conference will bring together stakeholders including government, academics, specialists, and private sector partners to discuss future economic, legal, social, and ethical issues relating to the development and deployment of artificial intelligence.

7.4 To complement its G7 work on artificial intelligence, Canada has also been working jointly with France to create an international study group that can become a global point of reference for understanding and sharing research results on artificial intelligence issues and best practices[14]. This initiative will work to create internationally recognized expertise and provide a mechanism for sharing multidisciplinary analysis, foresight and coordination capabilities in the area of artificial intelligence that is inclusive and multistakeholder in its approach. The group, comprised of government officials, joined by internationally recognized science, industry, and civil society experts, will analyze the scientific, technical and socioeconomic information that is needed to gain a better understanding of technological developments in artificial intelligence and identify the consequences of their use. Canada and France will set up a task force that will make recommendations on the scope, governance and implementation of the international study group that will be shared within the G7.

Other International Engagement

7.5 Canada participates in international fora such as the Organisation for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC) that are actively engaged in initiatives aimed at improving and expanding the global interoperability of privacy frameworks. Of particular relevance is current work between APEC and the European Commission aimed at exploring interoperability between the APEC Cross-Border Rules (CBPR) System and the EU's General Data Protection Regulation (GDPR). This work builds on earlier APEC/EU work that resulted in the development of a Referential that maps the requirements of the CBPR system with the EU Binding Corporate Rules. Canada is a member of the APEC working group that has been established to define a potential work program for renewed APEC/EU collaboration in the context of the GDPR.

8.0 Contact Information

8.1 Further information about any aspect of this report may be requested from Charles Taillefer, Director, Privacy and Data Protection Policy Directorate, Marketplace Framework Policy Branch,

[14] Further information on the Canada-France Statement on Artificial Intelligence is available at http://international.gc.ca/world-monde/international_relations-relations_internationales/europe/2018-06-07-france_ai-ia_france.aspx?lang=eng

Innovation, Science and Economic Development Canada at 235 Queen Street, Ottawa, Ontario, Canada K1A 0H5.

8.2 It is intended that future reports will be provided at regular intervals, approximately every six months.

Annex A - Further Information

This Annex offers further information and details relating to items presented in the Second Update Report, provided to the EC in November 2017.

Consequential Amendments to PIPEDA in 2004 arising from the Public Safety Act, 2002

1.1 In 2004, section 7 of PIPEDA was amended by the *Public Safety Act,* 2002, clarifying that an organization may collect and use information without the knowledge or consent of the individual for purposes of disclosure to a government organization only if it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs (PIPEDA, s. 7(1)(e)(i) and s. 7(2)(d)).

1.2 In terms of the basis for an organization to suspect, PIPEDA provides no definition for "suspicion". In the criminal law context, a "suspicion" refers to an expectation that a person is "possibly engaged in some criminal activity" (see *R v Kang-Brown* 2008 SCC 18, at para 75). The suspicion must be reasonable, which requires "more than a mere suspicion and something less than a belief based upon reasonable and probable grounds" (*Ibid.*). It is important to note that PIPEDA is not a criminal law statute and that the threshold for suspicion under criminal law must necessarily be high, given the fundamental rights engaged by criminal investigations. This high and objective standard may not necessarily apply to PIPEDA.

Access to Information Act

1.3 The *Access to Information Act* grants individuals a right of access to records under the control of government institutions. The Act allows Canadian government institutions to disclose records that contain personal information of a foreign citizen not present in Canada to this citizen's agent, provided two conditions are met: (1) the agent qualifies as a requester under the Act; and (2) the foreign citizen not present in Canada consents to the disclosure of their personal information to the agent.

1.4 *Qualification of the Agent under the Access to Information Act* - The agent that requests information under the Act must be a Canadian citizen, a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act*,[15] or an individual "present in Canada".[16]

1.5 *Consent to the Disclosure* - The right of access to records under the *Access to Information Act* is subject to exemptions and exclusions.[17] For instance, the Act sets a mandatory exemption on disclosure of records that contain personal information. However, this exemption gives government institutions the discretionary power to disclose such records with the consent of the individual to whom the personal information relates.[18] Therefore, a foreign citizen who is not present in Canada would have to consent to the disclosure of their personal information to the agent that made the request for access to information under the Act, prior to this disclosure.

[15] *Immigration and Refugee Protection Act*, S.C. 2001, c. 27.
[16] *Access to Information Act*, R.S.C., 1985, c. A-1, section 4. See also the *Access to Information Act Extension Order*, No. 1, SOR/89-207.
[17] *Access to Information Act*, section 4.
[18] *Access to Information Act*, paragraph 19(2)(a).

1.6 The consent of the foreign citizen must be in writing (signed and dated), and contain pertinent information to facilitate a federal institution to retrieve the relevant records. Specific information required includes; the foreign citizen's name, their date of birth, the name of the agent, the contact information of the agent, the signature of foreign citizen and the date the consent was signed.

1.7 *Access to Information Request* - The application fee for an access to information request is CAN$5.00 as per paragraph 7(1)(a) of the Access to Information Regulations. In accordance with Treasury Board Secretariat's Interim Directive on the Administration of the Access to Information Act, no other fees are charged to obtain access to an individual's personal information.

1.8 The Government of Canada is not responsible for, and does not regulate any fees agents may charge foreign citizens to represent them in making an access to information request. All requests are treated in the same manner by government institutions, regardless of whether they originate from a Canadian citizen or an agent representing a foreign citizen.

Application of the Charter within Canada

1.9 Although there have been some court decisions finding that the *Charter* does not apply to certain actions of Canadian officials outside Canada[19], we are not aware of any decisions suggesting that the *Charter* does not apply to actions within Canada that uniquely affect foreign citizens, nor of any case law suggesting that the term "everyone" in section 8 of the *Charter* excludes foreign citizens. It is emphasized however, that the *Charter* merely sets outer bounds on what the law may authorize Canadian officials to do. The laws themselves are a better source of information concerning the powers that Canadian officials may exercise within Canada.

Concept of "Reasonable Expectation of Privacy"

1.10 While the *Privacy Act* and PIPEDA apply to any personally identifiable information, section 8 of the *Charter* only applies to government actions that engage a reasonable expectation of privacy.

1.11 Whether a given action engages a reasonable expectation of privacy is evaluated according to the totality of the circumstances surrounding the action, with particular attention to a number of factors that have been identified by the courts.[20] Essentially, the question is whether the state action is one that interferes with the degree of privacy that an individual should be entitled to expect in a free and democratic society. To put it another way, actions that do not interfere with reasonable privacy expectations do not engage section 8 of the *Charter*. Examples of state actions that have been found not to interfere with a reasonable expectation of privacy have included situations where the individual has intentionally abandoned a privacy interest in the information (for example, by discarding a document in public[21]), where the information is publicly available (for example, a publicly-listed telephone number[22]),

[19] See, for example, *R. v. Hape* 2007 SCC 26, http://canlii.ca/t/1rq5n ; *Amnesty International Canada v. Canada (Chief of the Defence Staff)*, 2008 FCA 401 http://canlii.ca/t/21xc6 ; *Slahi v. Canada (Justice),* 2009 FCA 259, http://canlii.ca/t/25nn8

[20] These can include, but are not limited to: The relationship between the claimant and the party who holds the information; Whether the method of collection was invasive; The nature of the information collected; The regulatory context within which the collection occurs; and the relationship between the purpose for which the information was initially collected and the purpose of its disclosure.

[21] *R. v. Patrick* 2009 SCC 17, http://canlii.ca/t/231wj

[22] *R. v. Hutchings* (1996) 111 CCC (3d) 215 (BC C.A.), http://canlii.ca/t/1f07v

where the individual has provided truly voluntary and informed consent to the government action[23], or where the information, by its nature, does not reveal sensitive information about the individual.[24]

1.12 These factors are not, however, determinative. The analysis is always contextual and looks at the totality of the circumstances to determine the actual impact of a state action on privacy interests. Even the collection of information that is in theory publicly observable can intrude on a reasonable expectation of privacy where the police technique has a qualitative impact on privacy expectations – for example, the installation of a device to track the publicly-observable movements of a vehicle.[25] Also, collection of information that is not by nature sensitive can engage a reasonable expectation of privacy where it has the potential to reveal sensitive information, as with the link between a subscriber identity and an IP address associated with online activity.[26]

1.13 In the particular situation of collection of customer data, a key question is the relationship between the purpose of the disclosure and the purpose for which the information was originally provided. A customer does not abandon a privacy interest in information merely by handing it over to a third party (for example, a bank). A court will instead examine the relationship between the parties, including any applicable regulatory frameworks, in order to determine expectations as to how data will be handled. Generally, access by law enforcement, intelligence or regulatory agencies to customer data will engage a reasonable expectation of privacy and therefore require lawful authority.[27] Exceptions could include, for example, where the applicable contractual and/or regulatory frameworks provide that the information will be publicly available,[28] or where the organization holding the data was the victim of wrongdoing by the customer and reports a crime to police.[29]

1.14 The Department of Justice Canada has recently published Charterpedia, an online annotated resource explaining key case law relating to the *Canadian Charter of Rights and Freedoms*. The Charterpedia page regarding section 8 provides additional information on the concept of Reasonable Expectations of Privacy and may prove a useful resource.

Canadian Security Intelligence Service (CSIS)

1.15 In terms of investigative activities that require judicial authorization, CSIS would apply to the Federal Court of Canada for warrants under section 21 of the CSIS Act when investigative activities engage section 8 of the *Charter*. For example, CSIS would require a warrant to intercept an individual's communications. Two recent Federal Court decisions also provide examples of where CSIS would require a warrant:

- Regarding basic identifying information (2017 FC 1048), CSIS obtains detailed billing or subscriber information from communications service providers pursuant to judicial authorization from the Federal Court.

[23] *R. v. Borden*, [1994] 3 SCR 145, http://canlii.ca/t/1frrd
[24] *R. v. Tessling* 2004 SCC 67, http://canlii.ca/t/1j0wb; *R. v. Gomboc* 2010 SCC 55, http://canlii.ca/t/2dhlk
[25] See discussion in dissenting judgment of Laforest J. in *R. v. Wise* [1992] 1 SCR 527, http://canlii.ca/t/1fsdl
[26] *R. v. Spencer* 2014 SCC 43
[27] See, for an example relating to banking records, *R. v. Chusid* (2001) 57 OR (3d) 20, http://canlii.ca/t/1wc6v
[28] *R. v. Plant*, [1993] 3 SCR 281, http://canlii.ca/t/1fs0w
[29] *R. v. Fegan* (1993), 13 O.R. (3d) 88 (ON CA), http://canlii.ca/t/g16wp; See also *R. v. Cole* 2012 SCC 53 at para. 73, http://canlii.ca/t/ft969

- In its decision on the use of cell-site simulator technology by CSIS (2017 FC 1047), the Court determined that, while no warrant is required to use the technology for the purpose of attributing a cellular device to an individual, a warrant would be required to use it to geo-locate an individual's device.

1.16 Several conditions must be met for a judge to issue a warrant under section 21 of the CSIS Act. Among those is a requirement under section 21(2)(b) for CSIS to demonstrate that other investigative procedures have been considered, or that the urgency of proceeding with the requested activity is such that other methods would be impractical or would not result in obtaining the information. The jurisprudence around privacy as a fundamental right in Canadian society continues to evolve and, as such, the activities that require CSIS to obtain a warrant are changing as well.

1.17 More generally, CSIS' operational activities are conducted in accordance with the CSIS Act, Ministerial Direction and robust internal policies and procedures. All operational activity requires authorization, even if it does not require judicial authorisation under section 21 of the CSIS Act. Ministerial Direction provides the following fundamental principles to guide all of CSIS's operations:

- The rule of law must be observed;
- Operational activities must be reasonable and proportional to the threat;
- The greater the risk associated with a particular activity, the higher the authority required for approval;
- The rights and freedoms of individuals shall not be infringed unless the infringement is reasonable and proportional to the objective being pursued, in accordance with the following principles:
    - to employ the least intrusive operational techniques commensurate to the threat;
    - to minimize intrusions on human rights, including privacy, to the extent possible, and in accordance with Canadian law; and
    - to weigh the use of intrusive operational techniques against possible harm to civil liberties and to Canadian fundamental institutions.

1.18 Internal policies and procedures provide more specific direction to CSIS employees in conducting operations and investigations. Generally, policy documents outline requirements, including approval levels. Typically, the more intrusive an operational activity is, the higher approval authority that is required.

1.19 Pursuant to section 16 mandate of the CSIS Act, CSIS is authorized to assist the Minister of National Defence or the Minister of Foreign Affairs, within Canada, in the collection of information or intelligence relating to the capabilities, intentions or activities of foreign states and groups of foreign states, as well as any foreign citizen. CSIS may not collect information on a Canadian citizen, a permanent resident, or a Canadian company. CSIS only collects such information at the written request of the Minister of National Defence or the Minister of Foreign Affairs, and with the written consent of the Minister of Public Safety and Emergency Preparedness. The same obligations to obtain a warrant under section 21 of the CSIS Act apply to section 16.

1.20 In terms of safeguards related to data minimization and data retention, CSIS is authorized, pursuant to section 12 of the CSIS Act, to collect data, to the extent that it is strictly necessary, and analyze and retain information and intelligence on threats to the security of Canada. In accordance with robust internal policies and procedures, and supported by CSIS's information technology infrastructure, retained information may only be accessed on a "need to know" basis to further Service investigations. This applies to all information collected by CSIS. In issuing warrants, the Federal Court may impose additional conditions on the retention of information collected under those specific warrants.

1.21 In terms of the oversight and redress functions of the Security Intelligence Review Committee (SIRC), there are two types of complaints that may be submitted to SIRC: those filed pursuant to section 41 of the CSIS Act, and those filed pursuant to section 42. In the case of complaints submitted pursuant to section 41, these may relate to any "act or thing" done by CSIS. The person must first make a complaint to the Director of CSIS. If the person is not satisfied with the response they receive, or they do not receive a response within a reasonable timeframe (approximately 30 days), then they may file a complaint with SIRC. Once a complaint is received, SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith in order to undertake its investigation. CSIS may challenge the complaint on these grounds. However the decision to investigate rests with SIRC.

1.22 In the case of complaints submitted pursuant to section 42, these are related to the refusal or revocation of a security clearance. These have a similar process to section 41 complaints, with the exception that the complainant must submit the complaint within 30 days of receiving notice informing them that their security clearance has been denied or revoked.

1.23 SIRC issues a public Annual Report to Parliament which includes findings and recommendations. While these findings and recommendations, whether in relation to a review or a complaint file, are non-binding, the results of SIRC reviews and complaints routinely inform CSIS's policies and practices.

1.24 If a person is not satisfied with a SIRC decision, they may apply to the Federal Court for judicial review of that decision. As well, under the *Privacy Act*, an individual may make a complaint to the Privacy Commissioner of Canada in respect of any matter relating to the collection, retention or disposal of personal information by a government institution. That Act does not require the individual to have been personally affected by the collection, retention or disposal of personal information, and the Privacy Commissioner is also entitled to initiate a complaint in respect of a matter under the *Privacy Act*. If the individual who made the complaint is not satisfied with the decision of the Privacy Commissioner, the individual may then apply to the Federal Court for judicial review of the decision. While the *Federal Courts Act* permits an application for judicial review to be made by anyone directly affected by the matter, the Court has previously granted public interest standing in such cases. There are no special conditions for access to courts that apply to non-Canadians.

1.25 Given the nature and operational sensitivity of CSIS's investigations, there is no requirement for CSIS to inform individuals as to whether they have been subject to CSIS's investigative activities.