Government of Canada | Gouvernement du Canada

SECOND UPDATE REPORT ON

DEVELOPMENTS IN DATA PROTECTION LAW IN CANADA

Report to the European Commission November 2017

Canada

This publication is available online at http://www.ic.gc.ca/eic/site/113.nsf/eng/h_07661.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. Iu37-8/2-2018E-PDF

ISBN 978-0-660-27309-9

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

Table of Contents

1.0 Background

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).

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. Further engagement took place between Canadian and EC officials in a follow-up videoconference in July 2017.

1.4 On September 25, 2017, Innovation, Science and Economic Development Canada provided the European Commission will additional information, in the form of an Addendum to the first Update Report, as a follow up to the videoconference discussion during which EC officials sought clarification on several elements of the report on developments. The Addendum provided further information on the role and responsibilities of the Office of the Privacy Commissioner of Canada under the *Personal Information Protection and Electronic Documents Act*.

1.5 This report:

- further clarifies outstanding questions on the Canadian framework raised by EC officials during the videoconference on July 13, and
- outlines developments in Canada's data protection framework since the first update report prepared in May 2017.

2.0 Developments Related to Canada's Federal Privacy Laws

Data Breach Regulations under PIPEDA

2.1 In 2015 Canada's private sector privacy law, the *Personal Information Protection and Electronic Documents Act*, was amended to require organizations to report serious breaches of data security safeguards. These provisions will come into force after the completion of regulations which will provide further details on the statutory requirements such as minimum requirements for providing data breach reports to the Privacy Commissioner, notification to affected individuals, and the scope and retention period for data breach record-keeping.

2.2 A draft of the *Breach of Security Safeguards Regulations* was published on September 2, 2017 in the Canada Gazette Part I. The draft regulations can be found on the Canada Gazette website (see http://www.gazette.gc.ca/rp-pr/latest-publications-eng.html**)**

2.3 Innovation, Science and Economic Development Canada sought input and views on the draft regulations from interested parties until October 2, 2017. The feedback received is being used to inform the development of final regulations which are expected to be published in the Canada Gazette Part II, in the first half of 2018.

Parliamentary Committee Study of PIPEDA

2.4 On February 14, 2017 a Committee of the House of Commons began a study of PIPEDA as part of a series of legislative reviews pertaining to privacy protection in Canada. As part of its work, the Standing Committee on Access to Information, Privacy and Ethics heard from 65 witnesses representing private sector, civil society, academics, the Office of the Privacy Commissioner of Canada and other domestic and international data protection authorities. The Committee has sought the views and opinions of witnesses on key areas identified by the Privacy Commissioner of Canada as needing further examination, namely: the enforcement regime of PIPEDA; the consent model; the concept of right to be forgotten; the need for special rules for children online, and finally the importance of retaining EU adequacy. Though the study of PIPEDA is not considered a formal statutory review of the Act, the Committee has undertaken a comprehensive examination in these areas and is expected to issue a report of its findings and recommendations in the near future.

Canada's Anti-Spam Law (CASL)

2.5 Canada's Anti-Spam Law (CASL) provides for a private right of action (PRA). Under these provisions, individuals and organizations would have been able to bring a private right of action in court against individuals and organizations that they allege have violated the law. The PRA provisions were scheduled to come into force in July 2017, on the same day that Parliament was intended to review CASL (as per the Act). In order to promote legal certainty for numerous stakeholders claiming to experience difficulties in interpreting several provisions of the Act while being exposed to litigation risk, and recognizing that it is difficult for Parliament to review legislative provisions in the abstract, the coming into force date of the provisions was suspended on June 2, 2017, pending a legislative review of CASL.

2.6 On June 14th, 2017, the House of Commons designated the Standing Committee on Industry, Science and Technology (INDU) as the Committee that will undertake the parliamentary review of CASL. INDU held its first meeting in connection with this review on September 26, 2017.

National Security Consultations

2.7 On May 19, 2017, Canada released a report summarising "What We Learned" from the public consultations on the national security framework to provide Canadians with an overview of the input received during the consultations. In all, approximately 58,000 responses and 17,000 emails were received as part of these consultations. The information gathered during this consultation is being used to inform decisions regarding changes to Canada's national security framework. Most recently, it was used in the development of Bill C-59, the *National Security Act*, 2017, which is legislation currently before the Canadian Parliament that covers a wide range of measures aimed at enhancing accountability and transparency, fulfilling commitments to address former Bill C-51, and strengthening security and protecting rights.

Proposed Legislation - Bill C-59, the National Security Act, 2017

2.8 The Canadian government recently introduced legislation that enhances the government's oversight of national security agencies and proposes amendments to the Canadian Security Intelligence (CSIS) Act. Recognizing that this legislation is still subject to debate and consideration by Parliament in Canada, included below is a brief description of the proposed review schemes.

2.9 *National Security and Intelligence Review Agency* - The proposed National Security and Intelligence Review Agency (NSIRA) would enable comprehensive and integrated review of all national security and intelligence activities across the Government of Canada.

2.10 The NSIRA would replace the Security Intelligence Review Committee (SIRC) and the Office of the Communications Security Establishment Commissioner (OCSEC) (the review body responsible for Canada's Communications Security Establishment) and would also assume responsibility for the review of the RCMP's national security activities currently carried out by the Civilian Review and Complaints Commission (CRCC). It would also conduct reviews across departments and agencies engaged in security and intelligence activities.

2.11 The NSIRA would ensure that Canada's national security agencies are complying with legislation and that their actions are reasonable and necessary. It would have full and independent authority to determine what government activities to review. This would include the review of ongoing activities. Much like SIRC, it would also have unrestricted access to all documents (except for those subject to Cabinet Confidence).

2.12 Findings and recommendations from NSIRA would be provided to relevant Ministers through classified reports. It would also produce an unclassified annual report to Parliament summarizing the findings and recommendations provided to Ministers.

2.13 This new entity would complement the important work of the National Security and Intelligence Committee of Parliamentarians, which was recently created through Bill C-22. Having received Royal Assent, the Committee will be established in the coming months and CSIS, along with other federal departments and agencies, will be subject to its review. Together, they would provide comprehensive oversight of Canada's national security and intelligence activities.

2.14 *Intelligence Commissioner* - The Government of Canada proposes to create an Intelligence Commissioner (IC), a new oversight body with quasi-judicial status. The IC would have the mandate to review certain authorizations issued under the CSIS Act and the Communications Security Establishment Act, authorizations which are being proposed through Bill C-59. The IC would review the conclusions on the basis of which the authorizations are issued and would be responsible for their approval if deemed reasonable.

Recent Court Decisions

2.15 *Douez v. Facebook* - On June 23, 2017, the Supreme Court of Canada issued its decision in *Douez v. Facebook* on the enforceability of forum selection clauses in online contracts. Ms. Douez sought to initiate legal actions against Facebook in British Columbia for alleged breach of privacy activities. Facebook argued that she could not bring forward her case in British Columbia because when Ms. Douez created her account, she agreed to their terms of service, which include a forum selection clause, specifying that users must resolve any claims against the company in a court located in California. In its decision, the Supreme Court of Canada modified the common law test to determine whether a

Canadian court should override a forum selection clause, which they had established in the Pompey case. In this decision, the court recognized that, although the factors in Pompey have been interpreted and applied restrictively in the commercial context, the consumer context requires modification of these factors. The majority of the Supreme Court of Canada recognized that the enforceability of the forum selection clause may differ depending on the contractual context. The majority thus determined that courts should take into account public policy considerations relating to the gross inequality of bargaining power between the parties and the nature of the rights at stake when examining the enforceability of a forum selection clause in a consumer contract. The Supreme Court of Canada was of the view that public policy concerns relating to access to domestic courts are especially significant in this case given it concerns privacy as a fundamental right.

2.16 *Google Inc v Equustek Solutions* - In *Google Inc. v. Equustek Solutions Inc.*, the Supreme Court of Canada addressed three main issues:

i. Under what circumstances may a court order a search engine to block search results, having regard to the interest in access to information and freedom of expression, and what limits (either geographic or temporal) must be imposed on those orders?
ii. Do Canadian courts have the authority to block search results outside of Canada's borders?
iii. Under what circumstances, if any, is a litigant entitled to an interlocutory injunction against a non-party that is not alleged to have done anything wrong?

2.17 On the first issue, the Court determined that the interlocutory injunction is necessary to prevent irreparable harm as Datalink's business on the internet could not be carried out without Google's facilitation. The Court also determined that the order does not engage, on its face, freedom of expression values. Rather, it is aimed at preventing irreparable harm from the facilitation of the unlawful sale of goods resulting from Datalink's breach of several court orders. On the second issue, the Court determined that Canadian courts had authority to grant an injunction with worldwide effect because the problem, in this case, is occurring online and on a global scale. Therefore, without such reach, the interlocutory injunction would be unable to achieve its objectives in preserving Equustek's rights pending the outcome of the litigation. On the third issue, the Court determined that "the power to grant injunctions is presumptively unlimited, and injunctions aimed at maintaining order need not be directed solely at the parties involved in litigation."

2.18 *R. v. Orlandis-Habsburgo* - In *R. v. Orlandis-Habsburgo* the Ontario Court of Appeal revisited the Supreme Court of Canada decisions in R. v. Spencer, R. v. Gomboc and R. v. Plant. The case involved the routine sharing of energy consumption data between an electricity provider and the police. The Court found that, contrary to a situation where a company took specific data to the police with concerns that it revealed a crime had been committed, the informal nature of the information-sharing arrangement that Horizon had with the police did not comply with PIPEDA.

2.19 In this case the police and Horizon had an ongoing relationship when it came to the sharing of customer data. Justice Doherty noted that until the proceedings in this case commenced, Horizon had never refused a request from the police for information and found that this established that the police and Horizon were working in tandem. He noted this was important as this distinguished the situation from one where a company or whistleblower took specific data to the police with concerns that it revealed a crime had been committed. In its decision, the Court considered the exception in subparagraph 7(3)(c.1)(ii) of PIPEDA and found that the informal information-sharing arrangement

between the energy provider and the police failed to conform with that requirement. Furthermore, the Court found the exception in subparagraph 7(3)(d)(i) of PIPEDA, which allows an organization on its own initiative to disclose personal information to a government institution on "reasonable grounds to believe that the information relates to a contravention of the laws of Canada," does not permit informal information sharing with police.

2017 Annual Report to Parliament from the Office of the Privacy Commissioner of Canada (OPC)

2.20 In September 2017, the OPC's Annual Report to Parliament was issued. This report covers both the *Privacy Act*, which applies to the personal information handling practices of government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal private sector privacy law.

3.0 Clarifications from the May 2017 Update Report

3.1 This segment of the report includes additional information to supplement the May 2017 Update Report in response to EC requests for further clarification of various aspects. Section numbers from the May 2017 report have been included in the headings for reference purposes. In September 2017, additional information was also provided separately in an Addendum which expands upon the role and responsibilities of the Privacy Commissioner of Canada under the *Personal Information Protection and Electronic Documents Act*. These clarifications are based on current legislation and as such do not reflect ongoing initiatives, reviews or developments outlined in section 2 of this report.

Public Interest Exceptions to Consent under PIPEDA - Section 3.11

3.2 In general, PIPEDA requires an organization to obtain an individual's consent if it collects, uses or discloses his/her personal information to either another organization, a government institution or part thereof. However, the legislature recognizes that there are certain, limited circumstances in which an individual's right to privacy must be balanced against other fundamental rights and public interests. As such, the Act provides for exceptions to the general rule to allow organizations to disclose personal information either without an individual's consent or knowledge. The sections of PIPEDA that pertain to the issue raised relate to legislative exceptions allowing an organization to disclose an individual's personal information without his/her consent to another organization or government entity.

3.3 Subparagraph 7(3)(c.1)(iv) of the Act allows for disclosures of personal information by an organization to a government institution that has requested the information for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual. It allows for such a disclosure without requiring a warrant, subpoena or order. For a government institution to avail itself of this exception, it must satisfy the legal requirements of the Act.

3.4 First, the government institution should request the information and it should reflect its need for the information. Second, the request for disclosure must be for the explicit purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual. Lastly, the government institution should identify its lawful authority to obtain the information.

3.5 Paragraph 7(3)(d.3) of the Act is a permissive provision in that an organization, on its own initiative, may disclose personal information without consent for the purpose of preventing or investigating financial abuse. The disclosure can be made to a government institution, the individual's next of kin or his/her authorized representative. Such disclosures require that certain legislative conditions be met; the organization has reasonable grounds to believe

that the individual has been, is or may be the victim of financial abuse, the disclosure is made solely for purposes related to preventing or investigating the abuse, and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the ability to prevent or investigate the abuse.

3.6 This provision is intended to allow financial institutions to take measures to prevent financial abuse of elders, and other vulnerable customers, including for example, cases that involve unauthorized use of credit and debit cards, conflicting designations of powers of attorney, or misuse of powers of attorney, and joint bank accounts subject to abuse if the joint account holder uses the senior's money for their own purposes.

3.7 Subparagraph 7(3)(d.4) of the Act provides that an organization may disclose personal information without consent to a government institution, next of kin or authorized representative for the purpose of identifying individuals who may be ill, injured or deceased. If the individual is alive, the organization must inform him/her of the disclosure in writing and as soon as possible. The underlying purpose of this subparagraph is to allow for disclosures of personal information in situations that make it difficult or impossible to obtain consent such as accidents and disasters to assist in the identification of deceased, injured and ill individuals. For instance, by virtue of this subparagraph, dentists would be able to provide and disclose a patient's dental records to a government authority or to a family member to identify victims of a natural disaster.

Exceptions to Consent for Information Sharing under PIPEDA - Section 3.12

3.8 Paragraphs 7(3)(d.1) and 7(3)(d.2) of the Act, which respectively pertain to conducting private sector investigations and anti-fraud activities, provide that an organization can disclose personal information without consent to another organization, as distinct from a government institution. PIPEDA provides for conditions to be satisfied to lawfully make use of any of these exceptions.

3.9 Regarding paragraph 7(3)(d.1), the information being disclosed must be for the purpose of conducting an investigation into a breach of an agreement or a contravention of the laws of Canada or a province and, it must be reasonable to expect that informing the individual involved and obtaining their consent for the disclosure would compromise the investigation. It must pertain to a contravention or breach that has occurred, is occurring, or is about to occur. Information cannot be disclosed simply because the contract or agreement *may* be violated or contravened.

3.10 Examples of where this provision can be relied on include the investigation into professional misconduct by self-regulating professional association, such as Colleges of Physicians and Surgeons and Law Societies. A regulatory body may be required to look into illicit banking activities of a member against whom an allegation has been filed and, as such, the banking information would have to be obtained from a financial institution. Without these legislative exceptions, organizations such as these may not be able to question allegations of wrongdoing on the part of their members.

3.11 With respect to paragraph 7(3)(d.2), the information being disclosed without consent must be for the purpose of legitimate prevention, detection, or suppression of fraud that is likely to be committed, and, second, it must be reasonable to expect that informing the individual and obtaining their consent for the disclosure would compromise the ability to combat fraud. An example of the applicability of paragraph 7(3)(d.2) are investigations to detect financial crime or prevent fraud in the financial services sector, such as the work conducted by the Bank Crime Prevention Centre

and Investigation Office of the Canadian Bankers Association, and the Investigative Services division of the Insurance Bureau of Canada.

Consequential Amendments to PIPEDA in 2004 arising from the Public Safety Act, 2002 - Section 3.21

3.12 In 2004, PIPEDA was amended to permit the collection and use of personal information by organizations without the knowledge or consent of the individual, for the purpose of making a disclosure to government institutions for reasons of national security, the defence of Canada or the conduct of international affairs, or a disclosure required by law.

3.13 Under section 7(3) of PIPEDA, organizations were already authorized to disclose personal information without the individual's knowledge or consent to government institutions for reasons of national security, the defence of Canada, the conduct of international affairs, or where otherwise required by law (subsections 7(3)(c.1)(i); 7(3)(d)(ii); and 7(3)(i) of PIPEDA). The amendment to section 7(1) clarified that organizations may also collect and use personal information for the purpose of making these types of disclosures to government institutions.

3.14 The amendment was required in order to support the *Aeronautics Act*, which provides for Transport Canada officers, Royal Canadian Mountain Police (RCMP) or Canadian Security Intelligence Service (CSIS) designated persons, to require an air carrier or operator of a reservation system to provide them with passenger information under the air carrier's or operator's control, or that comes into their control within 30 days, for specified persons.

Transfers from private sector organizations to government institutions - Section 3.21

3.15 Paragraph 7(3)(c.1) of the Act allows for the disclosure of personal information from an organization to a government institution without the knowledge or consent of the individual in several circumstances; including where the government institution suspects that the information relates to national security, the defence of Canada or the conduct of international affairs.

3.16 To invoke this exception, the disclosure must have been requested by the government institution, the government institution must have indicated its lawful authority to obtain the information, and must have indicated that it suspects that the information relates to the national security, the defence of Canada or the conduct of international affairs.

3.17 Subparagraph 7(3)(d)(ii) also allows for disclosures without consent from an organization to a government institution for purposes related to national security and the defence of Canada. This provision allows for disclosures made on the initiative of the organization.

Powers of the Office of the Privacy Commissioner of Canada under the Privacy Act - Section 4.4

3.18 The *Privacy Act* establishes the Office of the Privacy Commissioner of Canada (Privacy Commissioner). The Privacy Commissioner is an Agent of Parliament whose mission is to protect and promote privacy rights. The Commissioner provides advice and information to individuals about protecting personal information. He also enforces two federal privacy laws that set out the rules for how federal government institutions and certain businesses must handle personal information.The Privacy Commissioner is an independent ombudsman with powers to investigate complaints, make recommendations respecting compliance with the Privacy Act, and issue reports to Parliament. The

Act creates a right for the Privacy Commissioner, upon consent of the individual, to apply to the Federal Court in respect of a refusal to provide that individual who has access rights under the Act with access to their personal information.

3.19 Sections 4 to 8 of the *Privacy Act* govern the collection, use, disclosure, retention and disposal of personal information by government institutions. The *Privacy Act* allows any individual, or their representative, to file a complaint with the Privacy Commissioner for an alleged breach of the obligations set by sections 4 to 8 and that relate to their personal information.[1] The Privacy Commissioner may also initiate a complaint if he is satisfied that there are reasonable grounds to investigate a matter under the *Privacy Act*.[2] In carrying out the investigation of any complaint under the *Privacy Act*, the Privacy Commissioner has the power to "summon and enforce the appearance of persons" before him and "compel them to give oral or written evidence on oath" and to produce documents, "in the same manner and to the same extent as a superior court of record".[3] The Privacy Commissioner also has the power to "enter any premises occupied by any government institution", converse in private with any person in those premises and "examine or obtain copies of or extracts from books or other records" in those premises.[4]

3.20 If the Privacy Commissioner finds that a complaint is well-founded, he will provide the government institution in question with a report containing the findings of the investigation, his recommendations and, if appropriate, will request that notice be given to him (within a specified period) of any action taken or proposed to be taken to implement the recommendations in the report or reasons why no such action has been or is proposed to be taken.[5] The Privacy Commissioner will also report the results of the investigation to the complainant.[6] In addition, section 37 of the *Privacy Act* provides the Privacy Commissioner with specific authority to carry out investigations to ensure compliance of government institutions with sections 4 to 8 of the *Privacy Act*. If, following such an investigation, the Privacy Commissioner considers that a government institution has not complied with any of sections 4 to 8, he will provide the government institution with a report containing the findings of the investigation and any recommendations that he considers appropriate.[7] Section 37 allows the Privacy Commissioner to review and report on the performance of government institutions in meeting the requirements of the *Privacy Act* and related government policy in regard to the gathering, handling and protection of personal information. Such monitoring is an essential part of ensuring the protection and privacy of personal information under the *Privacy Act*.

3.21 If the Privacy Commissioner is of the view that a government institution has failed to take adequate remedial action, he may communicate his finding in a report to Parliament. This may be done in the annual report to Parliament or, if the matter is sufficiently urgent or important, in a special report.[8] In practice this is rarely necessary: in 2016, the Privacy Commissioner recognized that "in the vast majority of cases, government departments do eventually agree to implement [his] recommendations".[9] Anyone directly affected by the decision of a government institution to collect, use

[1] See paragraphs 29(1)(a) and (h) and subsection 29(2) of the *Privacy Act*.
[2] See subsection 29(3) of the *Privacy Act*.
[3] See paragraph 34(1)(a) of the *Privacy Act*.
[4] See paragraphs 34(1)(d) to (f).
[5] See subsection 35(1) of the *Privacy Act*.
[6] See subsection 35(2) of the *Privacy Act*.
[7] See subsection 37(3) of the *Privacy Act*.
[8] See sections 38 and 39 of the *Privacy Act*.
[9] The Privacy Commissioner made this statement in a March 10, 2016 appearance before the Standing Committee on Access to Information, Privacy and Ethics. The text of the Commissioner's statement is available online: https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_20160310/ (last consulted on October 25, 2017).

or disclose personal information under the *Privacy Act* may challenge the lawfulness of the government decision through judicial review under section 18.1 of the *Federal Courts Act*.

Access to personal information - Section 4.5

3.22 The *Privacy Act* provides Canadian citizens, permanent residents, and by extension, inmates, and individuals present in Canada, a right of access to their personal information that is held by a federal government institution that is subject to the Act.

3.23 The *Access to Information Act* (ATIA) establishes a right of access to information in records under the control of a federal government institution that is subject to the ATIA.[10] This right of access applies to Canadian citizens and permanent residents and has been extended to individuals who are present in Canada and all corporations that are present in Canada.[11] A foreign citizen who is not present in Canada may access information, including their personal information, through a third party who is present in Canada. The foreign citizen would have to provide their consent to this third party.

3.24 In such a scenario, the third party would submit an access request to a government institution, and the proof of consent of the foreign citizen to make the request for their personal information, for records containing the personal information of the foreign citizen. The government institution responding to the request may disclose any record that contains the foreign citizen's personal information to the requester if the foreign citizen consents to the disclosure.

Concepts of a "reasonable expectation of privacy", "reasonable grounds to believe" - Sections 5 and 6

3.25 As discussed in section 5 of the May 2017 Update Report, jurisprudence under the *Canadian Charter of Rights and Freedoms* imposes certain constitutional requirements on state actions that engage privacy interests. The concept of a "reasonable expectation of privacy" is used to determine whether the protections of s. 8 apply to a given state action. As discussed in Section 6 of the same report, the concept of "reasonable grounds to believe" is a defined burden of proof employed to determine whether the requirements to authorize a search have been met. As requested, what follows is a more detailed discussion of these two concepts.

3.26 Reasonable expectation of privacy - S. 8 of the *Canadian Charter of Rights and Freedoms* provides protection against unreasonable searches and seizures. The Supreme Court of Canada has defined as a "search" any state action that engages a reasonable expectation of privacy.[12] The concept of a "reasonable expectation of privacy" is therefore employed to determine whether, as a threshold matter, the protections of s. 8 are engaged. The degree of this privacy expectation is then used in the balancing exercise to determine whether a law authorizing a search is reasonable – i.e. whether it is justifiable in light of the state's objective, taking into account any safeguards provided for in the law.

3.27 While the concept was initially borrowed from American jurisprudence under the Fourth Amendment,[13] it since has developed its own meaning, and own analysis, in Canadian caselaw under the *Charter*. In contrast to the protections provided by the *Privacy Act*, s. 8 will not govern *every* action that involves the collection, use or disclosure of information about an individual, but only those that engage a reasonable expectation of privacy.

[10] See subsection 4(1) of the *Access to Information Act* (ATIA).
[11] See subsection 4(1) of the ATIA and section 2 of *Access to Information Act Extension Order, No. 1*.
[12] *Hunter et al. v. Southam Inc.*, [1984] 2 SCR 145 ("*Southam*")
[13] *Katz v. United States* (1967) 389 U.S. 247 (U.S.S.C.)

3.28 The existence and extent of a reasonable expectation of privacy is determined by examining the totality of the circumstances surrounding the state action.[14] This test is guided by four lines of inquiry:[15]

i. an examination of the subject matter of the search;
ii. a determination as to whether the claimant had a direct interest in the subject matter;
iii. an inquiry into whether the claimant had a subjective expectation of privacy in the subject matter; and
iv. an assessment as to whether this subjective expectation of privacy was objectively reasonable.

3.29 The first inquiry, into the subject matter of the search, is aimed at determining the nature of the privacy interests at stake in a given situation, as well as focusing the rest of the analysis. The Supreme Court of Canada has identified three broad "spheres" of privacy that can be implicated by government action, although these spheres may overlap. These include personal privacy (the right of individuals not to have their bodies touched or explored), territorial privacy (the idea that certain places, such as dwellings, attract heightened privacy interests), and informational privacy[16] (the idea that individuals can expect privacy in respect of certain information).

3.30 The second inquiry examines the nature of the individual's relationship with the subject matter of the search. A claimant must demonstrate that his or her own privacy interest was breached, as opposed to the interests of third parties.

3.31 The third inquiry examines whether the individual had a subjective expectation of privacy in the subject matter of the search. For example, an individual will likely not have a subjective expectation of privacy in information that has been made public (for example, a listed telephone number). The existence of a subjective expectation of privacy is, however, not determinative. Privacy is a normative concept, and the focus of the analysis of reasonable expectations of privacy is what an individual *should* be entitled to expect in a free and democratic society.[17]

3.32 The fourth inquiry involves looking at a variety of factors to determine whether it would be objectively reasonable for an individual to expect privacy in the context of the particular situation. Although there is no exhaustive list of factors, relevant ones in the context of access to customer data can include the following:

- *Whether the subject matter of the search was in the hands of third parties and, if so, whether these parties had an obligation of confidentiality*. For example, a request to a bank for an individual's banking records will engage a reasonable expectation of privacy.[18]
- *Whether the method of the "search" was invasive.* For example, covert interception of ongoing communications is considered particularly intrusive.[19]
- *The nature of the information collected*. Since s. 8 is aimed at protecting a "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."[20] This includes information which tends to reveal intimate details of the lifestyle

[14] *R. v. Edwards*, [1996] 1 SCR 128 at para. 45
[15] *R. v. Cole* 2012 SCC 53
[16] Intrusions on informational privacy can result from a wide variety of actions, including certain instances of information sharing and electronic intercepts. A "search," for s. 8 purposes, is not limited to a physical search.
[17] *R. v. Tessling* 2004 SCC 67 ("*Tessling*") at para. 42.
[18] *Del Zotto v. Canada*, [1997] 3 FCR 40 (FCA).
[19] *R. v. Tse* 2012 SCC 16 ("*Tse*") at para. 17; *R. v. TELUS Communications Co.*, 2013 SCC 16.
[20] *R. v. Plant*, [1993] 3 SCR 281 at 293.

and personal choices of the individual.[21] Thus, for example, heat emanations from a building will not attract a reasonable expectation of privacy because of the limited information they reveal,[22] while subscriber information associated with an IP address linked to online activity will do so because of its potential to reveal sensitive information.[23]

- The context in which the "search" occurs. For example, compliance inspections and document requirements in a highly regulated industry will engage a lower expectation of privacy than searches for criminal purposes, and so will require fewer safeguards.[24]
- The nature of the relationship between the purpose for which information was initially collected and the purpose for which it was subsequently disclosed. Since individuals can generally expect that confidential information will be used for the purpose for which it was provided, subsequent use of that information for an unrelated purpose can engage an REP.[25]

3.33 *Reasonable grounds to believe* - "Reasonable grounds to believe" is the standard commonly used in federal legislation governing judicial preauthorization of searches in Canada.[26] It is interchangeable with the standard of "reasonable and probable grounds" and equivalent to the phrasing of "probable cause" in the American *Bill of Rights*.[27] Under the *Criminal Code*, for example, to grant a search warrant, a judicial officer must have reasonable grounds to believe that an offence has been committed and that there is evidence to be found at the place to be searched.[28] Under the *Canadian Security Intelligence Service Act*,[29] the granting of a warrant must be based on reasonable grounds to believe that the use of a particular investigative technique is necessary to investigate a threat to the security of Canada, or to perform other functions under the Service's mandate.

3.34 With some exceptions, the inclusion of a statutory condition requiring an officer to establish the existence of reasonable grounds for a search is a constitutional requirement for laws authorizing searches in the criminal context.[30] Thus, a law authorizing a search that would intrude on a well-defined privacy interest without requiring the officer to meet the standard of "reasonable grounds to believe" would generally be contrary to section 8 of the *Charter*.[31] The lower standard of "reasonable grounds to suspect" is used for certain searches that intrude on diminished privacy interests, such as the use of sniffer dogs.[32]

3.35 *Application of the "reasonable grounds to believe" standard* - The Supreme Court of Canada has established that the standard of reasonable grounds to believe is one of "credibly based probability" or "reasonable probability."[33] Reasonable grounds to believe will exist where there is an objective basis for the belief which is based on compelling

[21] *Ibid.*
[22] *Tessling*.
[23] *R. v. Spencer* 2014 SCC 43.
[24] *British Columbia Securities Commission v. Branch*, [1995] 2 SCR 3.
[25] *R. v. Dyment,* [1988] 2 SCR 417 at para. 30-31.
[26] "Reasonable grounds to believe" is also used as a standard in a number of other legal contexts, such as for decisions to arrest an individual, certain decisions relating to immigration, and certain administrative and regulatory decisions. It is a well-understood burden of proof in Canadian law.
[27] *Baron v R*, [1993] 1 SCR 416 at paras 54, 55; *Southam* at para 43.
[28] *Criminal Code*, R.S.C. 1985, c. C-46, s. 487(1).
[29] *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23, s. 21(2)(a).
[30] *R. v. Kang-Brown*, 2008 SCC 18 at para. 146; *Southam* at 167-168.
[31] *Ibid*.
[32] *Ibid.*
[33] *Baron* at para. 54; *Southam* at para 43.

and credible information.[34] The standard is therefore higher than a reasonable belief in the *possible* existence of relevant evidence or a reasonable belief that evidence *may* be uncovered in the search.[35] Reasonable grounds to believe requires more than a suspicion or possibility, but less than proof on a balance of probabilities.[36]

3.36 The Supreme Court has held that the application of the reasonable grounds test requires a subjective and objective assessment of the facts.[37] First, the officer must subjectively believe that there are reasonable grounds justifying the actions taken and, second, it must be objectively established that reasonable grounds do in fact exist.[38] In other words, is there sufficient evidence to support the officer's subjective belief?[39]

3.37 The totality of the circumstances – all of the facts and indicia available to the officer at the time – should be considered to determine whether reasonable grounds exist.[40] In applying the objective component of the lower "reasonable grounds to suspect" standard, the Supreme Court held that the existence of reasonable grounds should be judged based on the circumstances that the police were aware of or should have been aware of at the time the search was executed and not on facts that came to light afterward.[41]

3.38 In short, to meet the standard of "reasonable grounds to believe," an assessment of all of the facts by the reviewing tribunal must lead to the conclusion that the officer's subjective belief in a state of affairs justifying the search is objectively reasonable.[42] As discussed in the May 2017 Update Report, the absence of such grounds where they are required renders a search illegal and unconstitutional, and gives rise to a potential remedy under s. 24 of the *Charter*.

Canadian Security Intelligence Service (CSIS) - Section 6.16

3.39 The Canadian Security Intelligence Service (CSIS) is Canada's domestic security intelligence agency. Its activities must be carried out in accordance with the *Canadian Security Intelligence Service Act* (*CSIS Act*), which contains requirements for the collection, retention, and disclosure of information. CSIS must also conduct its activities in accordance with the *Canadian Charter of Rights and Freedom* and the *Privacy Act*, among other legislation.

3.40 CSIS' primary role is to investigate activities suspected of constituting threats to the security of Canada (as defined in section 2 of the *CSIS Act*), and to report on these activities to the Government of Canada. This function is carried out in accordance with the requirements of s.12 of the *CSIS Act*, which prescribes minimum requirements for the collection of information by CSIS, and states the following:

*"The Service shall collect, by investigation or otherwise, **to the extent that it is strictly necessary**, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada." [Emphasis added]*

[34] *Mugesera* at para. 114.
[35] *Southam* at para 42.
[36] *Mugesera v. Canada (Minister of Citizenship and Immigration)* 2005 SCC 40 ("*Mugesera*") at para. 114. See also *R. v. Shepherd* 2009 SCC 35 ("*Shepherd*") at para 23; *R v Debot*, [1989] 2 SCR 1140 at para 54.
[37] *Tse* at para 33; *R. v. Bernshaw,* [1995] 1 SCR 254 ("*Bernshaw*") at para 62; *R v Storrey*, [1990] 1 SCR 241 ("*Storrey*")at paras 16, 17.
[38] *Tse* at para 33; *Bernshaw* at para 62; *Storrey*, at paras 16, 17.
[39] *Shepherd* at para 3.
[40] *Ibid*. at paras 21, 23.
[41] *R v Chehil*, 2013 SCC 49 at para 34, [2013] 3 SCR 220.
[42] *Shepherd* at para 22.

3.41 CSIS is also authorized to conduct investigations for the purpose of providing security assessments to federal and provincial government departments, or advice to Ministers. For example, CSIS may advise the Ministers responsible for the *Immigration and Refugee Protection Act* and *Citizenship Act* on matters relating to the security of Canada to assist in the determination of admissibility of particular individuals to Canada and applications for citizenship.[43]

3.42 CSIS is only authorized to collect, retain or disclose information in accordance with the *CSIS Act*. While other legislation, such as the *Security of Canada Information Sharing Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), contain provisions authorizing the disclosure of information to CSIS by third parties, they do not alter or expand CSIS' ability to collect, which remains at all times subject to the requirements of the *CSIS Act*. In all cases, the requirements in the *CSIS Act* must be met before CSIS can collect the information.

3.43 CSIS may not collect, analyze or retain information unless there exists, at a minimum, "reasonable grounds" for suspecting that the activity constitutes a threat to the security of Canada. For investigative activities that are considered more intrusive, the Service must obtain prior judicial authorization (s.21 *CSIS Act*). Such an application for judicial authorization (or warrant) is heard *ex parte*, meaning the subject of the investigation is not present during the hearing. Allowing the subject to be present would be injurious to Canada's national security, given that sensitive investigative techniques would be revealed. Moreover, the purpose for which the information was collected (i.e., to investigate threats to the security of Canada) would be at risk of being revealed to the subject of the investigation.

3.44 Several conditions must be met for a judge to issue a warrant under s.21 of the *CSIS Act*, including that there must be reasonable grounds to believe a warrant is required to enable the Service to investigate a threat to the security of Canada.

3.45 CSIS discloses information in accordance with s.19 of the *CSIS Act*, which authorizes the disclosure of information for specific purposes, including for the performance of its duties and functions under the Act, or the administration or enforcement of the Act. CSIS may also disclose information where it may be used in the investigation or prosecution of an alleged offence, to the Minister of Foreign Affairs where the information relates to the conduct of the international affairs of Canada, and to the Minister of National Defence where the information is relevant to the defence of Canada.

Security Intelligence Review Committee (SIRC) - Section 6.19

3.46 The *CSIS Act* contains other requirements that govern CSIS' activities, which are related to accountability and review. To name a few, CSIS must obtain the approval of the Minister of Public Safety and Emergency Preparedness prior to applying to the Federal Court for a warrant. The Minister issues Ministerial Direction on any matter deemed appropriate. This direction serves as additional requirements as to how the Service fulfills its mandate. The Minister also approves CSIS entering into arrangements or cooperation with domestic and foreign partners. The *CSIS Act* provides for a rigorous review mechanism by the Security Intelligence Review Committee (SIRC).

3.47 *Security Intelligence Review Committee (SIRC)* - SIRC was established in 1984 as an independent, external review body that reports to the Parliament of Canada on the operations of CSIS. Its main functions as defined in the *CSIS Act*

[43] Section 15 authorizes the Service to conduct investigations as are required for the purpose of providing security assessments or advice and should be read in conjunction with ss.13 and 14 of the *CSIS Act*.

are to carry out in-depth reviews of CSIS' activities, conduct investigations into complaints, and certify the CSIS Director's Annual Report to the Minister. SIRC is completely independent of CSIS and at arm's length from Government. It consists of up to five part-time appointed members who serve on a fixed-term basis, supported by full-time staff comprised of an Executive Director and a dedicated team of lawyers, researchers, and other professionals. In conducting its reviews, SIRC has the authority to examine all information under CSIS' control, with the exception of Cabinet Confidences, and can also meet with CSIS officials. SIRC reviews CSIS's activities to provide assurances to Parliament and to Canadians that CSIS has acted in accordance with the law in performing its duties and functions.

3.48 SIRC's reviews for any given year assess a range of CSIS activities. This approach helps to ensure that over time, the Committee has a comprehensive understanding of the Service's activities. Each review usually includes findings or recommendations. Although these are not binding in nature, CSIS is expected to clearly indicate whether it agrees or disagrees. SIRC's findings and recommendations can also lead the Service to amend its internal policies and procedures.

3.49 SIRC examines through a quasi-judicial hearing presided over by a Committee Member, assisted by staff. Complaints can be made by "any person", and can relate to "any act or thing done by the Service" as described in the *CSIS Act*, the decision of another Government department to deny a required security clearance, or referrals from Immigration, Refugees and Citizenship Canada, or from the Canadian Human Rights Commission in cases where the complaint relates to the security of Canada. As part of the process, SIRC releases as much information as possible to the complainant, who has an opportunity to make representations. SIRC then makes findings and recommendations to the Government.

3.50 The results of SIRC's reviews of CSIS' operations are summarized in its Annual Report. This report is tabled in Parliament, usually in the fall and is edited to protect national security and personal privacy. The Director is also required to issue a classified report to the Minister on a yearly basis with respect to CSIS' operational activities. A copy of this report is also given to SIRC, which is required to certify to the Minister regarding CSIS' compliance with the *CSIS Act* and Ministerial Directives, including whether the activities mentioned in the Report involved any unreasonable or unnecessary use of powers. This function complements the assessments conducted by SIRC as part of its review work.

4.0 Further Information and Reports

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

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