Government of Canada | Gouvernement du Canada

Fourth Update Report on Developments in Data Protection Law in Canada

Report to the European Commission December 2018

Canada

This publication is available online at http://www.ic.gc.ca/eic/site/113.nsf/eng/h_07664.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. Iu37-8/4-2019E-PDF

ISBN 978-0-660-29318-9

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

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 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 the EC with the first in a series of biannual reports that outline key developments in Canada's data protection framework[1].

1.4 The EC's monitoring obligation was reaffirmed in May 2018 through the application of Article 45(4) of the General Data Protection Regulation (GDPR), which requires the Commission, on an ongoing basis, to monitor privacy-related developments in Canada that could affect the functioning of the existing adequacy decision. Recognizing that this monitoring activity continues, as part of the evaluation and review of the GDPR, which is to include an examination of existing adequacy decisions, which occurs every four years, beginning in May 2020, the present report:

- outlines developments in Canada's data protection framework since the third update report prepared in June 2018, and
- provides further information, in an Annex, on items of interest raised by EC officials during the videoconference held on September 12, 2018.

2.0 Developments Related to Canada's Private Sector Privacy Law

Breach of Security Safeguards Provisions and Regulations under PIPEDA

2.1 On November 1, 2018, new provisions in the *Personal Information Protection and Electronic Documents Act* (PIPEDA) related to breach of security safeguards came into force, along with the breach of security safeguards regulations. As such, PIPEDA now requires organizations to notify affected individuals, and to report to the Office of the Privacy Commissioner (OPC), all breaches that pose a real risk of significant harm to affected individuals. Organizations must also maintain records of any data breach they become aware of and provide them to the OPC upon request. Organizations that knowingly fail to comply with these obligations will be subject to fines. For example, organizations that willfully fail to notify individuals of a breach that creates a real risk of significant harm could face fines of up to CAN$100,000 per individual not notified. These new requirements are intended to provide individuals

[1] The series of biannual reports to the EC are available at http://www.ic.gc.ca/eic/site/113.nsf/eng/home

with an ability to protect themselves from harm resulting from a breach, and as an incentive for better data security safeguards on the part of organizations. The government has been actively engaging stakeholders in recent months in order to increase awareness of the new data breach obligations under PIPEDA.

2.2 The OPC has developed an overview of the new obligations associated with a breach of security safeguards. The OPC guidance document provides information for business on the mandatory reporting of breaches of security safeguards including what breaches have to be reported to the OPC, notices to affected individuals, as well as record keeping obligations.

Canada's Anti-Spam Legislation

2.3 On July 11, 2018, the Canadian Radio-television and Telecommunications Commission (CRTC) took enforcement action against the installation of malicious software through online ads under Canada's anti-spam legislation (CASL). The CRTC has issued Notices of Violation to Datablocks and Sunlight Media for allegedly aiding in the installation of malicious computer programs (malware) through the distribution of online advertising. The companies are required to pay CAN$100,000 and CAN$150,000 respectively, in administrative monetary penalties as a result of the investigation.[2]

2.4 On October 4, 2018 the CRTC signed a Memorandum of Understanding[3] with the Body of European Regulators for Electronic Communications (BEREC) to form a cooperative relationship. Through this memorandum, both agencies will support their respective efforts to address current and future regulatory challenges in Canada and Europe as well as to develop collegial working relationships. They will focus on a number of broad themes, including next generation access and broadband development, consumer protection, education and empowerment, network neutrality, open Internet and market competition. The CRTC and BEREC intend to carry out their cooperative activities for a period of two years, which could be extended for a further two years.

2.5 On November 5, 2018, the CRTC issued Compliance and Enforcement Information Bulletin 2018-415[4], which provides general compliance guidelines and best practices for stakeholders with respect to section 9 of CASL. The bulletin discusses the CRTC's general approach to section 9 and provides examples of parties to whom this section may apply and activities that could result in non-compliance. It also proposes measures for managing associated risks. Sections 6 to 8 of CASL prohibit the sending of commercial electronic messages without consent, altering transmission data in electronic messages in the course of a commercial activity without consent, and installing a computer program on another person's computer in the course of a commercial activity without consent. Section 9 of CASL addresses ways in which persons may contribute to contraventions of sections 6 to 8 of CASL without committing the violations directly.

[2] The Investigation can be found at https://crtc.gc.ca/eng/archive/2018/vt180711.htm and the associated press release is online at https://www.canada.ca/en/radio-television-telecommunications/news/2018/07/crtc-issues-250000-in-penalties-to-combat-malicious-online-advertising.html

[3] Text of the MOU can be found at https://crtc.gc.ca/eng/internet/berec.htm

[4] CRTC Bulletin 2018-415 is available at https://crtc.gc.ca/eng/archive/2018/2018-415.htm?_ga=2.144851056.536770588.1541431232-781512184.1525446427

3.0 Legislative Initiatives

Bill C-59, An Act respecting national security matters, 2017

3.1 The Canadian government has introduced legislation under Bill C-59, *An Act respecting national security matters*[5] that would enhance accountability mechanisms for national security agencies, and amend the powers of the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE). 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, in May 2018. In December 2018, the Bill was referred to the Senate Standing Committee on National Security and Defence for study.

3.2 The Bill proposes a National Security and Intelligence Review Agency (NSIRA) which would replace and enhance the review functions of the Security Intelligence Review Committee (SIRC) and the Office of the Communications Security Establishment Commissioner (OCSEC). Currently, Canada's national security review bodies operate separately, with each responsible for one intelligence agency. Under Bill C-59, NSIRA will be able to review national security activities of any government department or agency that has a national security function, including CSIS, CSE, Global Affairs Canada, the Canadian Border Services Agency, and Public Safety Canada. This significantly expands the scope of governmental activity that is subject to review and enhances the ability of Canada's national security review system to follow information as it flows between departments and agencies that have activities related to national security. In addition, Ministers will be able to refer activities that relate to national security or intelligence undertaken by their department or agency to NSIRA for review. NSIRA will investigate complaints against CSIS and CSE and will also investigate complaints on the conduct of the RCMP when those complaints are based on issues relating to national security.

3.3 The proposed NSIRA's complaints process will function much like that of its predecessor agency, SIRC. In terms of the process for an individual to submit a complaint to NSIRA[6], the procedure will remain substantially the same. With respect to CSIS and CSE, the complainant must first make a complaint to the organization. If they are dissatisfied with the response, or if they have not received a response within a reasonable time period, they may submit a complaint to NSIRA.

3.4 In addition to its complaint function, NSIRA may review any activity relating to national security or intelligence, and must review the implementation of all ministerial directions provided to CSIS and CSE or other departments when the direction relates to national security and intelligence. These directions serve as high level instructions to departments and agencies and guide the implementation of any department or agency's activities. After a review is complete, NSIRA may make any findings or recommendations it deems appropriate, including with respect to compliance with the law or ministerial direction, or the reasonableness and necessity of the exercise of powers by a government department.

[5] Further information on Bill C-59, *An Act respecting national security measures*, is available at http://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=9057418

[6] Any individual may make a complaint to NSIRA regarding national security actions taken by a Canadian government department or agency, whether or not they are resident in Canada. The process for complaints is the same regardless of nationality.

3.5 NSIRA will publish a public annual report on its activities that year, including unclassified versions of NSIRA's findings and recommendations, providing transparency and public oversight of the activities of government departments and agencies. If, in the course of a review, NSIRA believes that an activity related to national security and intelligence is not in compliance with the law, it must submit a report to the Minister responsible.

3.6 In 2017, the *National Security and Intelligence Committee of Parliamentarians (NSICOP) Act* was enacted, creating a multi-party committee that reviews the legislative, regulatory, policy, administrative and financial framework for national security and intelligence. NSICOP's mandate does not include the investigation of complaints. The Committee focuses on overarching issues dealing with how Canada's national security departments and agencies deliver on their mandates. The Committee may also review any activity that relates to national security or intelligence, unless that activity is part of an ongoing operation or would be injurious to national security.

Bill C-21, An Act to amend the Customs Act

3.7 In June 2016, the Canadian government introduced legislation to amend the *Customs Act* under Bill C-21, *An Act to amend the Customs Act.*[7] The Bill authorizes the CBSA to collect personal information on any person who is leaving, or has left, Canada at all land ports of entry. In addition, it requires that every person who is leaving Canada must, if requested to do so by an officer, present themselves to an officer and answer any questions the officer asks. The Bill amends the Act to authorize the disclosure of customs information to an official of the Department of Employment and Social Development for the purpose of administering or enforcing the *Old Age Security Act* (in addition to the *Employment Insurance Act*). Finally, it amends the Act to authorize officers to require that goods that are to be exported from Canada be reported and examined despite any exemption under the Act. On October 23, 2018, Bill C-21 passed Second Reading in the Senate and was referred to the Standing Senate Committee of National Security and Defence. The Bill provides the legislative authority for the collection of personal information in accordance with section 4 of the *Privacy Act* and prescribes the retention period.

Bill C-58, *An Act to amend the Access to Information Act and the Privacy Act and to make consequential amendments to other Acts*

3.8 On June 19, 2017, the Government introduced legislation to amend the *Access to Information Act* (ATIA) and make consequential amendments to the *Privacy Act.* Bill C-58 represents the first phase of a two-phased approach to reviewing the federal ATIA. The second phase, to modernize the Act, will include a full review of the Act to commence within one year of this legislation coming into force. The legislation proposes new requirements for the proactive publication of a broad range of information that apply to 265 federal government institutions, as well as the Prime Minister's Office, ministers' offices and administrative bodies that support Parliament and the courts. The legislation also proposes to transform the Information Commissioner's role from that of an ombudsperson to an authority with the legislated ability to make an order regarding the processing of requests, including the release of

[7] Further information on Bill C-21, *An Act to amend the Customs Act*, is available at http://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=8355229

records. It also provides the Information Commissioner with the ability to consult the Privacy Commissioner regarding the application of the exemption under the ATIA that requires federal institutions to refuse to disclose records that contain personal information. A review of the ATIA would also be required every five years.

3.9 The legislation would amend the *Privacy Act* to maintain consistency between the two Acts regarding reporting requirements, sharing of request processing services and the Governor in Council's authority to update the Schedule of government institutions subject to the Act. The current version of the Bill was passed by the House of Commons on December 6, 2017, and is now before the Senate.

Bill C-76, Elections Modernization Act, 2018

3.10 On April 30, 2018, the Government introduced the *Elections Modernization Act*[8], which proposes to amend the *Canada Elections Act* and other Acts to update Canada's electoral and political systems and address issues posed by the digital age, including concerns about the collection and use of data by political parties. 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. On October 22, 2018, the Standing Committee on Procedure and House Affairs reported the Bill back to the House of Commons, with amendments that would require online platforms to publish registries of partisan and elections advertising placed on their platforms. The Bill subsequently passed third Reading on October 30, 2018 and was referred to the Senate where it is now being studied by the Standing Senate Committee on Legal and Constitutional Affairs.

4.0 Parliamentary Committee Activities

Study of Breach of Personal Information Involving Cambridge Analytica and Facebook

4.1 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, the Committee issued an interim report on its study[9]. The Committee resumed its work On September 25, 2018 and intends to make additional recommendations in its final report once the study is complete.

Senate Report on Automated Vehicles

4.2 On January 29, 2018, the Senate Standing Committee on Transportation and Communication released its report, *Driving Change: Technology and the Future of the Automated Vehicle*, following a study on the regulatory and technical issues related to the deployment of connected and automated

[8] Further information on Bill C-76, the *Elections Modernization Act*, is available at http://www.parl.ca/LegisInfo/BillDetails.aspx?Language=E&billId=9808070

[9] Further information on the Committee's Study of the Breach of Personal Information Involving Cambridge Analytica and Facebook is available at http://www.ourcommons.ca/Committees/en/ETHI/StudyActivity?studyActivityId=10044891

vehicles (CAVs), which the Committee began in March 2016. The report contains sixteen recommendations on issues related to CAVs, including several related to privacy protection such as assessing the need for privacy regulations specific to CAVs. The Government Response[10] to the Senate Committee's report was tabled on July 27, 2018 and largely concurs with the Committee's privacy-related recommendations and notes the complementary study of PIPEDA by the House of Commons[11]. The Government also committed to work with stakeholders and partners, including the Office of the Privacy Commissioner, to develop an industry-specific code of best practices for privacy protection.

5.0 Office of the Privacy Commissioner Activities

Administrative

5.1 Earlier this year, the federal Privacy Commissioner made several announcements to indicate that the Office of the Privacy Commissioner has adopted a new organizational structure.[12] This new framework is based on two program areas - Compliance and Promotion. The Compliance Program focuses on addressing existing privacy compliance issues through a variety of enforcement activities to ensure violations of the law are identified and remedies are recommended. This will include investigations into complaints filed by individuals as well as a shift towards more proactive enforcement, such as Commissioner-initiated investigations or audits. The Promotion Program is aimed at individuals, to inform them of their rights and how to exercise them, and also at organizations, to bring organizations into greater compliance with federal privacy laws. This includes the development and promotion of practical information and guidance; reviewing and commenting on Privacy Impact Assessments (PIAs); and, proactively working with government and industry in an advisory capacity, to better understand and mitigate any privacy impacts related to new technologies such as big data, artificial intelligence and the Internet of Things.

Annual Report to Parliament

5.2 On September 27, 2018, the Office tabled its 2017-18 Annual Report to Parliament on PIPEDA and the *Privacy Act*[13]. In the report, the Commissioner noted ongoing investigations into a number of recent high profile privacy breaches, including those involving Cambridge Analytica and Facebook, Uber, and Equifax.

Online Reputation/Google

5.3 In January 2018, the OPC published its *Draft Position on Online Reputation*[14] as part of a public consultation process related to privacy and online reputation which indicates that the Office is of the

[10] Available at https://sencanada.ca/content/sen/committee/421/TRCM/reports/MinisterGarneau_GovResp_b.pdf
[11] See House of Commons Standing Committee on Access to Information, Privacy, and Ethics study of PIPEDA Towards Privacy by Design: Review of the *Personal Information Protection and Electronic Documents Act* and the associated Government Response to the report.
[12] Further information is available from the Office of the Privacy Commissioner of Canada 2018-19 Departmental Plan, tabled in Parliament on April 16, 2018 https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/planned-opc-spending/dp-index/2018-2019/dp_2018-19/
[13] The Report is available at https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201718/ar_201718/
[14] The draft policy position is available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/

view that the indexing of webpages and display of search results by search engines constitutes activities captured by PIPEDA. However, there is currently some uncertainty as to this interpretation of the law in this regard. In the context of an investigation involving an individual who alleges that Google is contravening PIPEDA, the Office has decided to apply to the Federal Court in order to seek clarity with respect to the applicability of PIPEDA.

5.4 On October 10, 2018, the Office of the Privacy Commissioner filed a Notice of Application in Canada's Federal Court to seek clarity on whether Google's search engine is subject to federal privacy law. More specifically, the application for reference asks whether Google's search engine service collects, uses or discloses personal information in the course of commercial activities and is therefore subject to PIPEDA. It also asks whether Google is exempt from PIPEDA because its purposes are exclusively journalistic or literary. The OPC has announced that investigations into complaints related to de-indexing requests will be stayed pending the results of the reference. The Office will also await the court's views before finalizing its position on online reputation.

Collection of Financial Information by Statistics Canada

5.5 On October 31, 2018 the Privacy Commissioner opened an investigation into Statistics Canada following complaints related to its collection of personal information from private sector organizations. Statistics Canada is working on new ways to understand consumers online, household production, intangible investment, and the evolving social and environmental issues in an increasingly digitalized world. The *Statistics Canada Act* provides legal authority for data collection, and the use of the data is strictly for statistical purposes and subject to strong legislative protections. As the matter was of interest to the Senate Standing Committee on Banking, Trade and Commerce, in connection with an ongoing study on the present state of the domestic and international financial system, the Privacy Commissioner, and officials from Statistics Canada, were invited to appear before the Committee[15].

Privacy Commissioners' Resolution on the Electoral Process

5.6 In September 2018, Canada's Information and Privacy Ombudspersons and Commissioners issued a joint resolution on *Securing Trust and Privacy in Canada's Electoral Process*[16]. In the Resolution, Federal, Provincial, and Territorial Privacy Commissioners of Canada urge their respective governments to ensure Canadian law, at all levels, carries meaningful privacy obligations for political parties. It calls on governments to pass legislation that: requires political parties to comply with globally recognized privacy principles; ensures Canadians have a right to access the personal information held about them; and provides for independent oversight to verify and enforce privacy compliance by political parties. The Resolution relates to Bill C-76 (*Elections Modernization Act*) which will require registered federal political parties to develop privacy policies and publish them online.

[15] Further information is available at https://sencanada.ca/en/Committees/BANC/NoticeOfMeeting/505782/42-1
[16] Further information is available at https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_180913/

6.0 Other Items of Interest

National Data Strategy

6.1 The Clerk of the Privy Council has released a Data Strategy Roadmap for the Federal Public Service[17] that is intended to support the strategic use of data by Government while protecting citizens' privacy. While not all data have privacy implications, the Strategy indicates that where they do, departments and agencies should incorporate privacy by design and engage early with the Office of the Privacy Commissioner. The roadmap is aimed at aligning internal government efforts to use data more strategically and complements other ongoing work, including national consultations on digital and data transformation (see below).

National Digital and Data Consultations

6.2 On June 19 2018, the Minister of Innovation, Science and Economic Development, launched public consultations on digital and data transformation focused on the areas of "Unleashing Innovation," "The Future of Work," and "Trust and Privacy." The National Digital and Data Consultations included an online portal for all Canadians to provide their input. The process concluded in October 2018 following national online public consultations and a series of roundtable discussions in cities across Canada. The government intends to release a "what we heard" report shortly. The results of the consultations will guide legislative changes related to privacy, as well as other marketplace frameworks.

Artificial Intelligence

6.3 In the context of its 2018 G7 Presidency, Canada continues to advance work internationally on artificial intelligence. Further to the commitment made by G7 Innovation Ministers during their Ministerial Meeting on *Preparing for Jobs of the Future*, Canada hosted a G7 Multistakeholder Conference on Artificial Intelligence on December 6, 2018 in Montreal, which built upon the G7 Innovation Ministers' Statement on Artificial Intelligence, and the G7 Leaders' *Charlevoix Common Vision for the Future of Artificial Intelligence*. This conference brought together over 150 artificial intelligence leaders from across the G7 including government officials, academics, civil society, research institutions, private sector partners and experts to discuss how to enable the responsible adoption of artificial intelligence, with a particular focus on fostering inclusion in artificial intelligence development and deployment, reducing barriers to innovation and enhancing market confidence, fostering accountability in artificial intelligence and promoting greater societal trust, and the future of work and skills for the modern economy – all with a view to building upon a common vision of human-centric artificial intelligence.

6.4 On December 6, 2018, Canada's Prime Minister and France's Secretary of State for Digital Affairs announced the mandate for the International Panel on Artificial Intelligence (IPAI). The IPAI will foster international collaboration to advance a shared understanding of artificial intelligence issues and to support and guide the responsible adoption of artificial intelligence that is human-centric and grounded in human rights, inclusion, diversity, innovation and economic growth. Canada and France will, over the

[17] The data strategy is available at https://www.canada.ca/en/privy-council/corporate/clerk/publications/data-strategy.html

coming months, invite international, like-minded partners to join them in shaping the IPAI into a global reference point for artificial intelligence.

6.5 The government has begun to utilize machine learning technologies to improve public services and programs. For example, to assist with the growing volumes of temporary resident applications Immigration, Refugees and Citizenship Canada is utilizing predictive analytics and implementing models to help officers identify applications that are routine and straightforward for faster processing, to triage files that are more complex for a more thorough review, and to detect fraud or other malfeasance in certain lines of business. This advanced analytics project is based on a strong foundation of ethics and privacy throughout the development process, as well as multiple Privacy Impact Assessments. Additional protocols to help ensure a thorough and unbiased assessment have been implemented.

Internet of Things (IoT)

6.6 The Internet Society, in collaboration with the Canadian Internet Policy and Public Interest Clinic and ISED, has launched a Canadian Multistakeholder Process on Enhancing Internet of Things Security. The group has established several working groups to address three main themes:

- Product labelling
- Consumer education and awareness
- Network resiliency

While still in very early stages of its work, the Group is making steady progress towards a common set of voluntary standards. The Group intends for these standards to be compatible with other international standards or norms for IoT devices.

Other International Engagement

6.7 Canada continues to participate 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 the upcoming review of the OECD *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* ("Privacy Guidelines") and work between APEC and the European Commission aimed at exploring interoperability between the APEC Cross-Border Privacy Rules (CBPR) System and the EU's General Data Protection Regulation (GDPR). Canada will actively participate in the OECD advisory group of experts that is being established to support the review of the OECD Privacy Guidelines and is a member of the APEC working group that is defining a potential work program for APEC/EU collaboration in the context of the GDPR.

7.0 Contact Information

7.1 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.

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

Annex - Further Information

This Annex offers further information and details relating to items presented in the Third Update Report, provided to the EC in June 2018, which have not been covered in the body of this report.

Intelligence Commissioner

A1.1 Bill C-59 sets out the proposed oversight functions and responsibilities of the Intelligence Commissioner (IC). Under the proposed *Intelligence Commissioner Act*, the IC will be mandated to review the reasonableness of Ministerial decisions regarding the use of certain powers by the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE). The IC will be provided with all of the information that was before the Minister. The IC will then determine whether it was reasonable for the Minister to have made the authorization based on the supporting evidence.

A1.2 The IC will receive copies of all reports from the National Security and Intelligence Review Agency (NSIRA) and the National Security and Intelligence Committee of Parliamentarians (NSICOP) that relate to their duties and functions. The IC will provide copies of all of its decisions to NSIRA so that they are aware of what actions were deemed unreasonable.

A1.3 Under the *Intelligence Commissioner Act*, the IC is appointed for a term of five years, and has the exclusive authority to manage personnel to assist them in their duties. The IC provides copies of their decisions to Canada's national security oversight bodies, ensuring that they are appropriately informed.

A1.4 The IC would have a mandate to oversee the authorization of certain activities of CSIS and CSE and would be fully independent of government. The IC's role pertaining to CSIS would be limited to oversight of certain specific CSIS activities. Specifically his/her role is to:

- review and approve the Minister's decisions regarding classes of Canadian datasets that CSIS could collect (section 16 of the *IC Act*);
- review and approve authorizations of the Minister (or his/her delegate) for the retention of foreign datasets(section 17 of the *IC Act*);
- in exigent circumstances, to review and approve the authorization of the CSIS Director for the query of Canadian or foreign datasets(section 18 of the *IC Act*); and
- review and approve the Minister's decisions regarding classes of activities that could be undertaken pursuant to the authorization scheme for acts or omissions that would otherwise constitute offences.

The IC would assess the reasonableness of the decision of the Minister (or delegate) or CSIS Director to authorize such activities. In regards to CSE, the IC would review and assess Ministerial authorizations permitting foreign intelligence and cyber security activities. The IC will review the Ministerial authorizations to ensure they are reasonable, necessary, proportionate, and that appropriate privacy protections are in place.

A1.5 The Intelligence Commissioner process will provide a new layer of accountability for certain types of CSIS activities, notably activities for which a warrant is not required. The IC would assess the reasonableness of the relevant Minister's decision to authorize certain specified collection activities as follows:

- Foreign intelligence authorizations (sections 34(1) and 34(2), issued under section 26(1) of the CSE Act). These authorizations allow CSE to gather foreign intelligence through the global information infrastructure;
- Cybersecurity authorizations (sections 34(1) and 34(3) issued under section 27(1) or 27(2) of the CSE Act). These authorizations allow CSE, in order to protect the security of federal institutions, to access a federal institution's information infrastructure in order to protect it from unauthorized use or disruption; and
- CSIS activities pursuant to section 20.1(3), and CSIS activities related to datasets. These CSIS activities may also require a warrant, depending on the nature of the activity.

A1.6 Decisions concerning investigative activities subject to the section 21 warrant regime of the *CSIS Act* will not be subject to the additional review of reasonableness by the IC. Rather, the warrant regime and the functions of the IC are intended to be complementary/distinct oversight mechanisms. However, there may be some areas where both are engaged. For example, when executing a section 21 warrant, CSIS could apply to the Federal Court to retain information incidentally collected in the execution of the warrant to constitute a dataset. If authorized by the Court, such a dataset would then be subject to the section 11 datasets framework in Bill C-59, including specific oversight functions of the IC, as outlined above. It is important to note that CSIS is subject to review by SIRC and the NSICOP, and will be reviewed by the proposed NSIRA in Bill C-59.

Datasets under Bill C-59

A1.7 Bill C-59 also amends the *CSIS Act* to create a regime that provides for CSIS to collect, retain, query and exploit datasets that contain personal information that does not directly and immediately relate to activities that represent a threat to the security of Canada[18]. This provides CSIS with a capacity to further its investigations through the identification of links and trends that are not possible using traditional methods of investigation. The framework sets out three types of datasets: publicly available datasets; Canadian datasets, which predominantly relate to Canadians and persons in Canada; and foreign datasets, which predominantly relate to non-Canadians outside of Canada. Foreign datasets can only be retained if they meet the threshold that they are likely to assist CSIS in the performance of its duties and functions. Their retention must be authorized by the Minister (or delegate) and approved by the IC, for a period of up to five years. Access to foreign datasets is restricted to designated employees and subject to record-keeping and audit requirements. Overall, the proposed approach would provide a clear framework within which CSIS may undertake data analytics using datasets that are not directly threat-related while ensuring that appropriate safeguards and accountability mechanisms are in place to

[18] A proposed framework is available at https://www.canada.ca/en/services/defence/nationalsecurity/our-security-our-rights/proposed-csis-dataset-framework.html

protect privacy. NSIRA will have the authority to review all types of datasets subject to the regime. NSICOP will provide an additional accountability mechanism as part of its ongoing mandate to review Canada's national security activities.

Canadian Security Intelligence Service (CSIS)

A1.8 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. CSIS may also take measures to reduce the threat. Its activities must be carried out in accordance with the *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 Freedoms* and the *Privacy Act*, among other legislation, as well as Ministerial Direction and internal policies and procedures. All operational activity requires authorization, even if it does not require judicial authorization under section 21 of the *CSIS Act*. Ministerial Direction provides guidance to CSIS that the greater the risk associated with a particular activity, the higher the authority required for approval. It also provides guidance that the Service must employ the least intrusive operational techniques commensurate to the threat.

A1.9 In terms of the Security Intelligence Review Committee's (SIRC) current ability to remedy non-compliance with the *CSIS Act*, and Ministerial Direction, the Committee has the power to make findings and non-binding recommendations. These are sent to the Minister of Public Safety and Emergency Preparedness as part of classified reports. Unclassified versions are published in a public report once a year, providing transparency and public review of CSIS's activities. With respect to SIRC's complaints process, an individual may make a complaint to the Committee in accordance with the *CSIS Act*. Any individual, including non-Canadians, may submit a complaint to the SIRC. The process for complaints is the same regardless of nationality with the exception that non-Canadians outside of Canada may not benefit from the protection of the *Canadian Charter of Rights and Freedoms*. Complaints reports may also contain non-binding recommendations. Further, the federal Privacy Commissioner, when investigating a complaint concerning the activities of CSIS, has access to all information, with the exception of Cabinet Confidences.

Access to Data for National Security Purposes

A1.10 Data on EU individuals stored in Canada would only be accessed if it was relevant to a Canadian law enforcement or CSIS investigation, such as if an EU individual was suspected of committing a crime in Canada. Such access would be predicated upon compliance with applicable legal authorities, and restrictions governing lawful access to data, including a requirement for judicial authorization, depending on what data is being sought. Separately, CSE has a mandate to acquire and use information for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities. Under its assistance mandate, CSE may provide assistance to RCMP and CSIS during the course of an investigation to help solve technical challenges in accessing digital evidence or intelligence that has been lawfully obtained. This must be done in compliance with all relevant legal authorities and restrictions governing lawful access to data, including judicial authorizations.

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

A1.11 The following case law provides examples of decisions where the "reasonable suspicion test" was applied. However, there has not been relevant case law where this test was applied or discussed in relation to PIPEDA.

- *R. v. Mahmood,* [2008] O.J. No. 3922[19]
- *R. v. Merritt,* [2017] ONSC 366[20]
- *Ontario v. Bharath,* 2016 ONCJ 382[21]
- *R. v. Chehil,* 2008 NSSC 357[22]
- *Stevens v. SNF Maritime Metal Inc.,* 2010 FC 1137[23]
- *R. v. Devloo, [2015] ABQB 345*[24]

Access to Personal Information by Foreign Nationals

A1.12 The *Privacy Act* does not grant foreign citizens that are not present in Canada the right to make a request for their personal information under the control of federal government institutions.[25] As a result, the *Privacy Act* also does not provide such individuals with rights related to the right to request access to their personal information, which include the right to request correction, require that a notation be made reflecting a correction request but not made, and require that any person or body to whom the information has been disclosed be notified of the correction or notation.

A1.13 However, foreign citizens are able to access their personal information through the *Access to Information Act.* The *Access to Information Act* provides a right of access to government-held information to Canadian citizens, permanent residents, and individuals and corporations present in Canada. In addition, anyone outside of Canada may make an access request through a Canadian agent. The *Access to Information Act* prohibits the disclosure of a record requested under that Act if it contains personal information; however, such a record can be released if, among other things, the individual to whom it relates consents to the disclosure. Accordingly, in such cases, an agent located in Canada acting on behalf of a foreign national could make a request for various records under the ATIA pertaining to the foreign national, who in turn could consent to the disclosure of his or her personal information to the agent.

[19] https://www.canlii.org/en/on/onsc/doc/2008/2008canlii51774/2008canlii51774.html?autocompleteStr=R%20v.%20mahmood&autocompletePos=3#_Toc211144885
[20] https://www.canlii.org/en/on/onsc/doc/2017/2017onsc366/2017onsc366.html?autocompleteStr=R.%20v.%20Merritt%2C%202017%20ONSC%20366&autocompletePos=1
[21] https://www.canlii.org/en/on/oncj/doc/2016/2016oncj382/2016oncj382.html?autocompleteStr=Ontario%20v.%20Bharath%2C%202016%20ONCJ%20382&autocompletePos=1
[22] https://www.canlii.org/en/ns/nssc/doc/2008/2008nssc357/2008nssc357.html?autocompleteStr=%09R.%20v.%20Chehil%202008%20NSSC%20357&autocompletePos=1
[23] https://www.canlii.org/en/ca/fct/doc/2010/2010fc1137/2010fc1137.html?autocompleteStr=Stevens%20v.%20SNF%20Maritime%20Metal%20Inc.%202010%20FC%201137&autocompletePos=1
[24] *https://www.canlii.org/en/ab/abqb/doc/2015/2015abqb345/2015abqb345.html?autocompleteStr=R.%20v.%20Devloo%20&autocompletePos=1*
[25] *Privacy Act*, R.S.C. 1985, c. P-21.

Foreign Nationals Benefit From the Code of Fair Information Practices

A1.14 Foreign citizens not present in Canada benefit from protections set by the Code of fair information practices enshrined under sections 4 to 8 of the *Privacy Act*. These provisions set requirements on the collection (s. 4 and 5), use (s. 7), disclosure (s. 8) and retention and disposal (s. 6) of personal information. These provisions focus on government institutions' handling of personal information. They do not account for, or distinguish on the basis of, the citizenship status or geographical location of the individual to whom personal information relate. The requirements set by sections 4 to 8 are binding upon government institutions.

Oversight by Privacy Commissioner of Canada and Federal Court

A1.15 Because foreign nationals do not have a right to request access to their personal information under the *Privacy Act,* they cannot make a complaint to the Privacy Commissioner of Canada in respect of a refusal to access their personal information from a federal government institution. However, the improper handling (i.e. collection, use, disclosure, retention and disposal) of personal information by a government institution allows the individual to whom the personal information relates to file a complaint with the Privacy Commissioner of Canada,[26] including foreign citizens not present in Canada. If an investigation of the Privacy Commissioner of Canada reveals that a complaint is well-founded, the Commissioner can formulate a report with recommendations to government institutions and request that they give notice to the Commissioner within a specified time of "any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken".[27]

A1.16 Improper handling of personal information by government institutions also allows "anyone directly affected" to apply for judicial review under the *Federal Courts Act*.[28] This includes foreign citizens not present in Canada. The *Federal Courts Act* allows the Federal Court to "order a federal board, commission or other tribunal to do any act or thing it has unlawfully failed or refused to do or has unreasonably delayed in doing".[29] The Act also allows the Federal Court to "declare invalid or unlawful, or quash, set aside or set aside and refer back for determination in accordance with such directions as it considers to be appropriate, prohibit or restrain, a decision, order, act or proceeding of a federal board, commission or other tribunal".[30] The *Federal Courts Act* defines a "federal board, commission or other tribunal" as "any body, person or persons having, exercising or purporting to exercise jurisdiction or powers conferred by or under an Act of Parliament or by or under an order made pursuant to a

[26] *Ibid.*, para. 29(1)(a) and (h).
[27] *Privacy Act*, subsection 35(1).
[28] *Federal Courts Act*, subsection 18.1(1).
[29] *Ibid.*, paragraph 18.1(3)(a).
[30] *Ibid.*, paragraph 18.1(3)(b).

prerogative of the Crown", with exceptions.[31] There are precedents for engaging the Federal Court to review actions pertaining to sections 4 to 8 of the *Privacy Act* under the *Federal Courts Act*.[32]

[31] *Ibid.*, subsection 2(1). The exceptions relate to the Tax Court of Canada and its judges, provincial bodies and judges. For more information on the terms "federal board, commission or other tribunal" see paragraph 29 of *Anisman* v. *Canada (Border Services Agency)*, 2010 FCA 52.
[32] See *Sauvé* v. *Canada (Attorney General)*, 2016 FC 401, *Union of Canadian Correctional Officers/Syndicat des Agents Correctionnels du Canada Confédération des Syndicats Nationaux CSN (UCCO-SACC-CSN)* v. *Canada (Attorney General)*, 2016 FC 1289 and *Kelly A. O'Grady* v. *Attorney General of Canada*, 2017 FC 167.