



# Sixth Update Report on Developments in Data Protection Law in Canada

---

*Report to the European Commission December 2019*

This publication is available online at <http://www.ic.gc.ca/eic/site/113.nsf/eng/home>

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](http://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](mailto:ISED@canada.ca)

#### Permission to Reproduce

Except as otherwise specifically noted, the information in this publication may be reproduced, in part or in whole and by any means, without charge or further permission from the Department of Industry, provided that due diligence is exercised in ensuring the accuracy of the information reproduced; that the Department of Industry is identified as the source institution; and that the reproduction is not represented as an official version of the information reproduced or as having been made in affiliation with, or with the endorsement of, the Department of Industry.

For permission to reproduce the information in this publication for commercial purposes, please fill out the Application for Crown Copyright Clearance at [www.ic.gc.ca/copyright-request](http://www.ic.gc.ca/copyright-request) or contact the Web Services Centre mentioned above.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of Industry, (2020).

Cat. No. Iu37-8/6-2020E-PDF

ISBN 978-0-660-33942-9

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

# Contents

1.0	Introduction .....	1
2.0	Developments Related to Canada’s Private Sector Privacy Law.....	1
3.0	Legislative Initiatives .....	2
4.0	Parliamentary Committee Activities .....	2
5.0	Recent Court Decisions .....	3
6.0	Office of the Privacy Commissioner Activities .....	3
7.0	Other Items of Interest .....	6
8.0	Contact Information.....	7

## 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 officials provided the EC with the first in a series of biannual reports that outline key developments in Canada's data protection framework<sup>1</sup>.

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 fifth update report prepared in June 2019.

## 2.0 Developments Related to Canada's Private Sector Privacy Law

### *Personal Information Protection and Electronic Documents Act (PIPEDA)*

2.1 There are no statutory developments or amendments to the legislation since the last report.

### *Canada's Anti-Spam Legislation (CASL)*

2.2 The second annual CASL Performance Measurement Report 2018-2019 will be made available online.<sup>2</sup> The annual report provides an overview of the governance and compliance elements of CASL as well as statistical information from the Spam Reporting Centre.

2.3 There are no statutory developments or amendments to the legislation since the last report.

---

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

<sup>2</sup> Performance Management Reports are available at <https://www.fightspam.gc.ca/eic/site/030.nsf/eng/00019.html>

## 3.0 Legislative Initiatives

### *Coming into force of legislation containing national security review and oversight measures*

3.1 Bill C-59, the *National Security Act, 2017*, created a new review body, the National Security and Intelligence Review Agency, and a new oversight body, the Intelligence Commissioner. Both were established in July 2019. The National Security and Intelligence Review Agency (NSIRA) was established under the *National Security and Intelligence Review Agency Act*. It has the authority to review and report on the lawfulness, reasonableness and necessity of any government activity that relates to national security intelligence. NSIRA also investigates complaints made against the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE) as well as national security-related complaints made against the Royal Canadian Mounted Police. It also receives complaints on denials or revocations of security clearances. The Review Agency has unfettered access to all information, except Cabinet Confidences.

3.2 The Intelligence Commissioner was established under the *Intelligence Commissioner Act*. The Commissioner, who must be a retired judge of a superior court, provides enhanced oversight to certain intelligence and cyber security activities set out in legislation governing the CSE and CSIS. The Commissioner approves certain authorizations issued and determinations made by the Minister of National Defence and the Minister of Public Safety upon having reviewed their conclusions for reasonableness.

### *Reports from the National Security and Intelligence Committee of Parliamentarians (NSICOP)*

3.3 The National Security and Intelligence Committee of Parliamentarians (NSICOP) complements NSIRA's compliance-based review and conducts strategic-level reviews of NSI activities across the federal government. The NSICOP submitted to the Prime Minister their 2019 special report on the Department of National Defence and the Canadian Armed Force's collection, use, retention, and dissemination of information on Canadians. This special report and the Committee's second annual report are expected to be tabled in Parliament in early 2020.

## 4.0 Parliamentary Committee Activities

### *Study on Privacy of Digital Government Services*

4.1 On June 18, 2019 the House of Commons Standing Committee on Access to Information, Privacy and Ethics released the report on its study on digital government services<sup>3</sup> to understand how the government can improve services to Canadians while protecting their privacy and security. The Committee heard from thirty-three witnesses and received four written submissions. The Committee's report makes eight recommendations to the federal government that pertain to privacy and digital government services:

---

<sup>3</sup> The report is available at <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10583346/ethirp19/ethirp19-e.pdf>

1. Modernize the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* by adopting the Committee's recommendations regarding these acts in previous reports.
2. Commit to uphold data minimization, de-identification of all personal information at source when collected for research or similar purpose, and clarify the rules of consent regarding the exchange of personal information between government departments and agencies.
3. Work to inform Canadians about the coming shift to digital government and involve them in the design and development of infrastructure needed to deliver digital government services.
4. Work to ensure collaboration and information sharing between departmental and government agencies with respect to the implementation of digital government services in order to ensure effective deployment of these services on a large scale.
5. Promote the connection of various departmental databases to a digital backbone to allow for secure and controlled sharing of data.
6. Work to ensure that reliable, affordable Internet access is extended to rural and remote areas even as services are digitized in areas already serviced.
7. Consult with Indigenous peoples when developing digital government services.
8. Establish guiding principles relating to privacy, cybersecurity and digital literacy in smart city projects in partnership with provincial, municipal and Indigenous governments.

4.2 The Committee emphasized that the shift to digital government should not be at the expense of protecting the privacy of Canadians. The Government will consider the Committee's recommendations in the context of its ongoing work to review the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*.

## 5.0 Recent Court Decisions

There are no updates to report.

## 6.0 Office of the Privacy Commissioner Activities

### *Annual Report to Parliament*

6.1 In December 2019, the Office of the Privacy Commissioner (OPC) released its annual report for 2018-2019<sup>4</sup>. The report highlights the OPC's investigations into Facebook and Equifax and provides updates on key operational trends for the OPC. For example, the OPC has experienced a 500 percent increase in the number of incoming data breach reports since November 2018 when mandatory data breach reporting came into effect under PIPEDA. Of note, the OPC believes that part of the reason for dramatic increase is excessive caution and over-reporting by many businesses; for instance, the OPC found that 33% of the reports it had received by March 2019 did not actually meet the reporting threshold of "real risk of significant harm" required by the Act.

---

<sup>4</sup> [2018-19 Annual Report to Parliament on the \*Personal Information Protection and Electronic Documents Act\* and the \*Privacy Act\*](#)

6.2 The annual report also includes recommendations for reform of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the *Privacy Act*, in addition to the results of several high profile investigations under those Acts. In the report, the Commissioner suggests the starting point to legislative reform is to give new privacy laws a rights-based foundation. The Commissioner also calls for new enforcement mechanisms so that the Commissioner may issue binding orders and impose penalties for non-compliance with the law. The OPC also believes that PIPEDA should provide individuals with a private right of action.

#### *Online Reputation/Google*

6.3 On July 22, 2019, the Federal Court issued an [Order](#)<sup>5</sup> refusing to allow Google to expand the scope of the Reference to include constitutional questions. The Court did not accept Google's argument that the issue of constitutionality is "inextricably intertwined" with the Reference questions. The Court found that it is possible to answer the jurisdictional question, of whether PIPEDA applies to Google's search engine service, without answering the constitutional question relating to freedom of expression (s.2b) of the *Charter*. The jurisdictional question only asks whether PIPEDA applies, not whether it infringes Google's rights.

6.4 Therefore, the scope of the OPC's Reference before the Federal Court remains concerned with the two following questions:

- 1) Does Google, in the operation of its search engine service, collect, use or disclose personal information in the course of commercial activities within the meaning of paragraph 4(1)(a) of PIPEDA when it indexes web pages and presents search results in response to searches of an individual's name?
- 2) Is the operation of Google's search engine service excluded from the application of Part 1 of PIPEDA by virtue of paragraph 4(2)(c) of PIPEDA because it involves the collection, use or disclosure of personal information for journalistic, artistic or literary purposes and for no other purpose?

With the scope determined, the Court is now deciding on various motions to intervene and Google's motion to file additional evidence.

#### *Consultations on Transborder Data Flows under PIPEDA*

6.5 In April 2019, the OPC announced a consultation on transborder data flows<sup>6</sup> under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) proposing that organizations be required to obtain consent when transferring personal information to third parties for processing. In June 2019, the Office announced a reframing of its consultations<sup>7</sup>, with the publication of a reframed discussion

---

<sup>5</sup> <https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/419820/index.do>

<sup>6</sup> Further information on the consultations is available at <http://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transborder-dataflows/>

<sup>7</sup> The Announcement is available at [https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an\\_190611/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190611/)

document<sup>8</sup>, which included three additional questions for stakeholder input, and an extended deadline of August 6, 2019.

6.6 On September 23, 2019, the OPC concluded its consultation on transfers of personal information for processing, and [announced](#) that the 2009 *Guidelines for Processing Personal Data Across Borders*<sup>9</sup> “will remain unchanged under the current law”. The Guidelines were developed to explain how PIPEDA applies to transfers of personal information to a third party for processing, including a third party operating outside of Canada.

#### *Joint Resolution on Effective Privacy and Access to Information Legislation in a Data Driven Society*

6.7 In November 2019, a Joint Resolution from the Information and Privacy Ombudspersons and Commissioners across Canada was issued. The resolution, *Effective Privacy and Access to Information Legislation in a Data Driven Society*<sup>10</sup>, acknowledges that while legislative advances have been made in some Canadian jurisdictions, there is still a need to “enhance and establish consistent modernization” in order to better protect individuals. It calls on government to modernize access to information and privacy laws, specifically to put in place:

- a legislative framework to ensure the responsible development and use of artificial intelligence and machine learning technologies;
- all public and private sector entities engaged in handling personal information to be subject to privacy laws;
- Enforcement powers, such as legislating order-making powers and the power to impose penalties, fines or sanctions; and,
- the right of access should apply to all information held by public entities, regardless of format.

6.8 The Joint Resolution also served to reaffirm their commitment to collaborate, make recommendations to government, and to continue to study and make public how access and privacy laws impact all Canadians.

#### *International Conference of Data Protection & Privacy Commissioners (ICDPPC)*

6.9 At the 41<sup>st</sup> International Conference, held October 2019 in Albania, the OPC sponsored a Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising other Fundamental Rights<sup>11</sup>, which was adopted by members of the ICDPPC. The OPC also [co-authored a resolution](#) on cooperation between data protection authorities and consumer protection and competition authorities and co-sponsored four other resolutions from the event:

---

<sup>8</sup> The Reframed discussion document is available at <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/>

<sup>9</sup> The 2009 policy position on transborder data flows is available at [https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl\\_dab\\_090127/](https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/)

<sup>10</sup> The Joint Resolution 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\\_191001/](https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_191001/)

<sup>11</sup> The Resolution is available at <https://icdppc.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf>



- [Resolution on the promotion of new and long-term practical instruments and continued legal efforts for effective cooperation in cross-border enforcement](#)
- [Resolution to address the role of human error in personal data breaches](#)
- [Resolution on the Conference’s strategic direction \(2019-21\)](#)
- [Resolution on social media and violent extremism content online](#)

## 7.0 Other Items of Interest

### *Canada’s Digital Charter*

7.1 Following the federal election in October 2019, the Minister of Innovation, Science and Industry has been mandated to advance Canada’s Digital Charter and enhanced powers for the Privacy Commissioner. With respect to the set of proposals to modernize PIPEDA, outlined in the paper *Strengthening Privacy in the Digital Age*<sup>12</sup>, the government has recently engaged with a number of stakeholders to better understand their views on the proposals and to help define the options going forward. To date, a broad range of stakeholders, including business associations, private sector organizations including internet-based companies, civil society and academia have been consulted.

### *Open Banking Consultations*

7.2 In 2018, the Government announced it would undertake a review of open banking and appointed an [Advisory Committee on Open Banking](#)<sup>13</sup>. A public [consultation paper](#) was released in January 2019, and roundtable consultations were held to engage Canadians. The Advisory Committee has completed the first phase of the review and the Department of Finance is currently reviewing its findings.

### *Artificial Intelligence*

7.3 Canada’s Advisory Council on Artificial Intelligence, launched on May 14, 2019, convenes experts from industry and academia to inform the Government of Canada’s long-term vision for Canada on AI both domestically and internationally. The Advisory Council has struck a working group to consider and report on how to commercialize value from Canadian-owned AI and data analytics. A second working group will consider avenues to boost public awareness and foster trust in AI in order to better ground the Canadian discourse in a measured understanding of the technology, its potential uses, and its associated risks.

7.4 In August 2019, G7 Leaders acknowledged the work of Canada, France and partners to create a Global Partnership on AI (GPAI), which will be an expertise-based, multi-stakeholder organization dedicated to the responsible adoption of AI. Interested countries and partners – including the EU – continue to work together toward the launch of GPAI in early 2020, as well as the launch of the GPAI Secretariat to be hosted by the OECD.

<sup>12</sup> The paper is available at [https://www.ic.gc.ca/eic/site/062.nsf/eng/h\\_00107.html](https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html)

<sup>13</sup> The Advisory Committee on Open Banking was established by the Minister of Finance in September 2018.

7.5 Canada and France have announced that Centres of Expertise in Montreal and Paris will support the work of the GPAI Working Groups and will plan GPAI's annual Multi-stakeholder Experts Group Plenary meeting. The first Plenary will take place in Canada in fall 2020. In addition to supporting GPAI, the Centre of Expertise in Montreal – created in partnership with the Government of Quebec – will analyze measures for strengthening Canada's capacity to commercialize and adopt AI-related technologies.

#### *Standards Council of Canada*

7.6 The Canadian Data Governance Standardization Collaborative, established in May 2019 as part of Canada's Digital Charter, is a cross-sector coordinating body, consisting of representatives from industry, government, civil society, academia and standards organizations. Its objective is to accelerate the development of industry-wide data governance standards and specifications. A Steering Committee and working groups have been established to support the development of a roadmap that will take a life-cycle approach to data governance from data collection, through access and sharing and ending with data analytics and commercialization. The publication of the final Roadmap, expected late 2020, will be used to facilitate greater understanding of standardization priorities for data governance in Canada.

#### *International Engagement*

7.7 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. As part of this work, Canada continues to contribute to the review of the OECD *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*<sup>14</sup>, as a member of the OECD Privacy Expert Group, established to provide advice on the review of its implementation. With respect to APEC, Canada is a member of the Data Privacy Sub-Group that is updating the Cross-Border Privacy Rules (CBPR) System to reflect the updated *APEC Privacy Framework (2015)*<sup>15</sup>. In addition, Canada is participating in APEC/EU discussions aimed at updating the 2014 *Referential on Personal Data Protection and Privacy Requirements of BCR and CBPR*<sup>16</sup> and exploring the concept of certification as it relates to the GDPR and the CBPR.

## **8.0 Contact Information**

8.1 Further information about any aspect of this report may be requested from Charles Taillefer, Director, Privacy and Data Protection Policy Directorate, Marketplace Framework Policy Branch, Innovation, Science and Economic Development Canada at 235 Queen Street, Ottawa, Ontario, Canada K1A 0H5.

---

<sup>14</sup> See <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>

<sup>15</sup> See [http://publications.apec.org/Publications/2017/08/APEC-Privacy-Framework-\(2015\)](http://publications.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015))

<sup>16</sup> See [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp212\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf)

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