

Right2YourFace Coalition

Explainer: Private Sector Legislative Framework for Facial Recognition Technology in Canada

Author: Alessandra Puopolo

Article Citation: Alessandra Puopolo, "Explainer: Canada's Private Sector Legislative Framework for Facial Recognition Technology in Canada," (July 2023), online (pdf): *Right2YourFace Coalition* <right2yourface.ca/learn/private-sector-legislative-framework-for-facial-recognition-technology-in-cananda/>.

Article Link: <https://right2yourface.ca/learn/private-sector-legislative-framework-for-facial-recognition-technology-in-cananda/>

WHAT ARE THE KEY PRIVATE SECTOR LAWS THAT GOVERN FACIAL RECOGNITION TECHNOLOGY IN CANADA?

In Canada, there is no legislation that explicitly governs the use of facial recognition technology (FRT), and private companies are increasingly using FRT for a variety of purposes including: identity verification, fraud prevention, and to monitor consumer behaviour.¹ At the federal level, businesses engaging in commercial activities are governed by *the Personal Information Protection and Electronic Documents Act* (PIPEDA), which has not been substantially updated since its enactment in 2000.² While the federal government has recently proposed a series of new legislative reforms to

¹ Office of the Privacy Commissioner of Canada, *Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information & Privacy Commissioner for British Columbia*, [PIPEDA Findings #2020-004](#) (Ottawa: OPC, 2020); Office of the Information & Privacy Commissioner for British Columbia, *Investigation Report: Canadian Tire Associates Dealers' use of facial recognition technology*, ([British Columbia: BCIPC 17, 2023](#)); Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, [PIPEDA Findings #2021-001](#) (Ottawa: OPC, 2021).

² *Personal Information Protection and Electronics Documents Act*, [SC 2000, c 5 \[PIPEDA\]](#).

modernize Canada’s private sector privacy legislation, these reforms are unlikely to adequately protect individuals’ rights and personal information against the use of FRT.³

At the provincial level, several provinces have enacted legislation that is substantially similar to PIPEDA and have introduced increased legislative protection for individuals’ privacy rights.⁴ Significantly, in 2021, Quebec became the first jurisdiction in Canada to take legislative action to update its privacy legislation and include specific requirements on industry use of facial recognition technologies.⁵

FEDERAL LEGISLATION: THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

What are the key provisions of PIPEDA?

Enacted in 2000, PIPEDA governs how privacy sector organisations in Canada can collect, use, and disclose personal information in the course of commercial activity.⁶ Commercial activity has been applied and interpreted broadly to include social networking sites that use personal information for the purpose of enhancing users’ experience and organisations offering free services when consider in the context of their entire business activities.⁷ Under PIPEDA, personal information means “information about an identifiable individual” that is recorded in any form, including information

³ Christelle Tessono & Sonja Solomun, “How to Fix Canada’s Proposed Artificial Intelligence Act” (6 December 2022), online (blog): *Tech Policy Press* <techpolicy.press/how-to-fix-canadas-proposed-artificial-intelligence-act/> ; Michael Geist, “Why the Government Should Hit the Regenerate Button on its AI Bill” (19 April 2023), online (blog): *Michael Geist* <www.michaelgeist.ca/2023/04/why-the-government-should-hit-the-regenerate-button-on-its-ai-bill/>; “Joint Letter of Concern regarding the government’s response to the ETHI Report on Facial Recognition Technology and the Growing Power of Artificial Intelligence”, (June 2023) online: *Right2YourFace Coalition* <right2yourface.ca/open-letter/>; Christelle Tessono et al., “AI Oversight, Accountability and Protecting Human Rights: Comments on Canada’s Proposed Artificial Intelligence and Data Act” (November 2022) online (pdf): Cybersecure Policy Exchange <www.cybersecurepolicy.ca/aida/>.

⁴ Office of the Privacy Commissioner of Canada, “Provincial laws that may apply instead of PIEDA” (May 2020), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/>.

⁵ *An Act to modernize legislative provisions as regards the protection of personal information, SQ 2021, c 25.*

⁶ *PIPEDA*, *supra* note 2 at s 4.

⁷ Office of the Privacy Commissioner of Canada, “Interpretation Bulletin: Commercial Activity” (January 2017) online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_03_ca/>.

relating to an individual's age, name, ethnic origin, opinions, and medical records among others.⁸ Some of the key provisions of PIPEDA are:

- Principle 4.3 of Schedule 1 requires that organisations must obtain individuals' knowledge and consent when collecting, using, or disclosing their information.⁹ Moreover, section 6.1 stipulates that such consent is only valid if an individual "would understand the nature, purpose and consequences of the collection, use, or disclosure of the personal information to which they are consenting."¹⁰
- Section 5(3) of PIPEDA provides that notwithstanding valid consent, organizations can only use personal information for appropriate circumstances.¹¹ In its *Guidance on Inappropriate Data Practices*, the Office of the Privacy Commissioner of Canada (OPC) has outlined five no-go zones for data processing, including profiling that would lead to discriminatory treatment contrary to human rights law and purposes that would cause significant harm to an individual.¹²
- The OPC oversees compliance with PIPEDA and individuals in Canada may file a complaint with the office. While the OPC can conduct investigations and issue reports of its findings and recommendations, its decisions are not legally-binding.¹³

What are some of the issues with PIPEDA?

One of the most glaring issues with PIPEDA is that it has not been substantially updated for decades. With the advent of new technologies, specifically the growth of digital processes and artificial intelligence (AI) that have transformed how data is collected, used, and disclosed, Canada requires up-to-date private sector legislation specifically crafted with a view to address these developments.¹⁴

⁸ PIPEDA, *supra* note 2 at [s 2\(1\)](#); Office of the Privacy Commissioner of Canada, "PIPEDA in Brief" (May 2019) online: Office of the Privacy Commissioner <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/> [Privacy Commissioner, PIPEDA in Brief].

⁹ PIPEDA, *supra* note 2 at [Schedule 1, c 4.3](#).

¹⁰ *Ibid* at [s 6.1](#).

¹¹ *Ibid* at [s 5\(3\)](#).

¹² Office of the Privacy Commissioner of Canada, "Guidance on Inappropriate data practices: Interpretation and application of subsection 5(3)" (May 2018), online: Office of the Privacy Commissioner of Canada <www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/>

¹³ PIPEDA, *supra* note 2 at [ss 11-12](#).

¹⁴ Office of the Privacy Commissioner of Canada, "A Regulatory Framework for AI: Recommendations for PIPEDA Reform" (November 2020), online: Office of the Privacy Commissioner of Canada <<https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation->

PIPEDA does not distinguish between different types of personal information. In its current form, it does not prescribe the necessary specific and heightened protections for highly sensitive data, such as biometric information (e.g., facial images, fingerprints, etc.), including how and when such information can be used, collected, stored, and shared. Specific regulations are required to delineate no-go zones and ensure adequate disclosure for particularly invasive technologies such as FRT.¹⁵ Additionally, PIPEDA does not provide the OPC with necessary enforcement powers, such as the ability to perform proactive audits to ensure compliance with privacy legislation or to impose meaningful penalties for violations, such as fines and other penalties. Currently, such remedies can only be granted by the courts.¹⁶

PROVINCIAL AND TERRITORIAL LEGISLATION: A PATCHWORK

Provincial governments in Alberta,¹⁷ British Columbia,¹⁸ and Quebec¹⁹ have each enacted their own privacy laws to govern the private sector that are substantially similar to PIPEDA.²⁰ Additionally, many provinces and territories have their own health privacy legislation that regulates the collection, use, and disclosure of personal information in the healthcare sector, including healthcare providers, service providers, and agents.²¹ Despite these legislative frameworks, like their federal counterparts, most of these statutes are out of date and were enacted long before many of today's technologies, such as artificial intelligence, were substantially developed and deployed.

Legislative Developments: Quebec

In 2021, the Government of Quebec adopted new legislation (Law 25: *An Act to modernize legislative provisions as regards to the protection of personal information*) to modernize the province's privacy

[ai/reg-fw_202011/](#)> ; Ignacio Cofone, "Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report" (November 2020), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/>; Teresa Scassa, "PIPEDA reform should include a comprehensive rewrite" (2018), online (blog): *Teresa Scassa* <www.teresascassa.ca/index.php?option=com_k2&view=item&id=279:pipeda-reform-should-include-a-comprehensive-rewrite&Itemid=80&tmpl=component&print=1>.

¹⁵ Daniel Therrien, "Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020" (May 2021), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/>.

¹⁶ PIPEDA, *supra* note 2 at [ss 11-12](#); Office of the Privacy Commissioner of Canada, "Key recommendations for a new federal private sector privacy law" (May 2022) online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-news/news-and-announcements/2022/recs_c11/>.

¹⁷ *Personal Information Protection Act, SA 2003, c P-6.5*.

¹⁸ *Personal Information Protection Act, SBC 2003, c 63*.

¹⁹ *An Act respecting the protection of personal information in the private sector, CQLR, c P-39.1*.

²⁰ Privacy Commissioner, *PIPEDA in Brief*, *supra* note 8.

²¹ *Ibid.*

laws with many of the provisions entering into force in September 2023.²² The legislation will apply to organisations headquartered in Quebec, or those that hold personal information of Quebec residents. Significantly, these new amendments substantially update some protections for individuals' personal information, including biometrics. Under the new framework, businesses must notify the Commission d'accès à l'information du Québec (CAI) before deploying any biometric identification techniques, including FRT, and they must obtain individual's express consent before collecting biometric information.²³ The new legislation also prescribes increased fines for non-compliance, with financial penalties ranging from \$15,000 – 25 million or 4% of an entity's worldwide turnover for the fiscal year.²⁴ Notably, this legislation is the first of its kind in Canada. Additionally, the CAI has also prohibited entities from combining thermal cameras with FRT systems.²⁵

RECENT DEVELOPMENTS IN CANADA'S FEDERAL PRIVATE SECTOR PRIVACY LEGISLATION: BILL C-27

Bill C-27: An Overview

In June 2022, the Canadian government introduced Bill C-27: *Digital Charter Implementation Act, 2022*, that proposes to significantly update Canadian privacy legislation by repealing Part 1 of PIPEDA, would enact the *Consumer Privacy Protection Act*, and establish the *Personal Information and Data Protection Tribunal Act*.²⁶ Additionally, Bill C-27 seeks to develop a statutory framework for artificial intelligence through the *AI and Data Act (AIDA)*.²⁷ However, the proposed legislation is unlikely to adequately protect individuals' privacy, personal information, and related rights as it:

- does not engage with many of the recommendations outlined in the ETHI Report detailed in the next section below;
- was not drafted with adequate public consultation, including community advocates, researchers, and equity deserving groups;

²² *An Act to modernize legislative provisions as regards the protection of personal information*, [SQ 2021, c 25](#).

²³ *Ibid* s 45.

²⁴ *Ibid* s 91.

²⁵ Commission d'accès à l'information du Québec, *Enquête à l'égard de Héritage Ébénisterie Architecturale inc.*, [1023688-S](#) (14 June 2021).

²⁶ Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, [1st Sess, 44 Parl, 2022](#) (second reading and referral to committee 24 April 2023).

²⁷ *Ibid*.

- does not explicitly prohibit the use of FRT in certain circumstances (“no-go zones”) such as by police or industry to facilitate mass surveillance. In comparison other jurisdictions, such as the European Union have proposed such legislative constraints;
- is silent on special protections for sensitive personal information such as biometric data including faces, fingerprints, and vocal patterns. Instead, almost all types of data are treated the same;
- will only apply to high impact AI systems;
- focuses only on individual harms, rather than collective harms;
- lacks adequate and future-proof definitions of key terms such as artificial intelligence, and
- prioritizes the rights of businesses over individuals in Canada, permitting businesses to collect and use individuals’ information without their consent for certain activities.²⁸

ETHI Committee FRT & AI Study and Report

In 2022, the Standing Committee on Privacy and Ethics (ETHI) conducted public consultations and published a report reviewing the status of facial recognition technology and artificial intelligence in Canada.²⁹ Among its findings, the ETHI Committee recommended that the government should:

- require industries to publicly disclose their use of FRT (Recommendation 1);
- increase its investment in initiatives to study the impact of AI on various demographic groups, increase digital literacy, and educate Canadians about their privacy rights (Recommendation 8);
- explicitly define acceptable uses of FRT and prohibit other uses, including mass surveillance (Recommendation 11);
- implement the right to be forgotten, requiring services providers and other entities to delete user’s personal information after a set period of time (Recommendation 14);

²⁸ Tessonno & Solomun, *supra* note 3; Geist, *supra* note 3; Right2YourFace Coalition, *supra* note 3; Tessonno et al., *supra* note 3; Teresa Scassa, “Explaining the AI and Data Act” (21 March 2023), online (blog): www.teresascassa.ca/index.php?option=com_k2&view=item&id=369:explaining-the-ai-and-data-act&Itemid=80; Amanda Cutinha & Christopher Parsons, “Minding Your Business: A Critical Analysis of the Collection of De-identified Mobility Data and Its Use Under the Socially Beneficial and Legitimate Interest Exemptions in Canadian Privacy Law” (22 November 2022), online (pdf): Citizen Lab <citizenlab.ca/2022/11/a-critical-analysis-of-the-collection-of-de-identified-mobility-data/>.

²⁸ Office of the Privacy Commissioner of Canada, “Provincial laws that may apply instead of PIEDA” (May 2020), online: Office of the Privacy Commissioner of Canada <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/>.

²⁹ House of Commons, *Facial Recognition Technology and the Growing Power of Artificial Intelligence: Report of the Standing Committee on Access to Information, Privacy and Ethics (October 2022)* (Chair: Pat Kelly).

- implement an opt-in-only requirement for the collection of biometric data by private sector entities and prohibit collection as a requirement for service (Recommendation 15);
- strengthen the ability of the OPC to levy meaningful penalties for violations of PIPEDA (Recommendation 16);
- amend PIPEDA to prevent the capture of images from the internet and public spaces for use in FRT databases (Recommendation 17); and
- enact a moratorium on the use of FRT by industry until adequate legislation is in place (Recommendation 18).³⁰

Government Response and Looking Forwards

In February 2023, François-Philippe Champagne, the Minister of Minister of Innovation, Science and Industry, replied to the ETHI Committee’s report on behalf of the government.³¹ The reply did not adequately detail how the government intends to address many of the issues and recommendations raised in the report. Significantly, the government did not propose any significant adjustments to Bill C-27 that would have reflected the ETHI Committee’s recommendations. Overall, the government’s reply faltered in multiple key areas, including by failing to:

- engage with the calls for a federal moratorium on the use of FRT;
- assume a leadership role in responsible tech policy;
- update that current Treasury Board Directive on Automated Decision Making that regulates the use of FRT by federal agencies;
- engage with key stakeholders in developing Bill C-27; and
- ensure that Bill C-27 will protect individuals' privacy rights.

The proposed legislation was delayed in the 2023 Spring session of Parliament and will be reviewed by the Standing Committee on Industry and Technology in the Fall of 2023.³²

³⁰ *Ibid* at 3-6.

³¹ François-Philippe Champagne, “Government Response to the Sixth Report of the Standing Committee on Access to Information, Privacy and Ethics” (February 2023) online (pdf): *Government of Canada* <www.ourcommons.ca/content/Committee/441/ETHI/GovResponse/RP12190465/441_ETHI_Rpt06_GR/MinisterOfInnovationScienceAndIndustry-e.pdf>

³² “C-27”, online: *Parliament of Canada* <www.parl.ca/legisinfo/en/bill/44-1/c-27>