

Facial Recognition Through the Lens of National Legislations - Canada*

Leah West
(Carleton University)

ABSTRACT Canada currently lacks comprehensive federal legislation explicitly regulating the use of facial recognition technology (FRT) or biometric data more broadly. Apart from Quebec's 2001 Act, which establishes a legal framework for information technology and imposes specific requirements on biometric identification systems, the use of FRT across the country is governed primarily by general privacy laws. These laws constrain the collection and use of personal information but provide limited clarity on the use of FRT, especially by public authorities. The Supreme Court of Canada has yet to rule on whether such technologies engage constitutional privacy rights under the Charter, leaving the legal status of FRT in public spaces unsettled. This paper examines the existing legal frameworks and documents the known public uses of FRT in Canada. It explores privacy law in both private and public sectors, including investigations into FRT use in retail and biometric screening at Canadian borders. It also analyzes the evolving legal debate around Charter protections against state surveillance. The paper concludes by considering how forthcoming privacy and AI legislation may shape the future governance of biometric technologies in Canada.

KEYWORDS: Facial Recognition Technology - Biometric Data - Canadian Privacy Law

TABLE OF CONTENTS: 1. Introduction. – 2. Private Sector Privacy Framework. – 3. Public Sector Privacy Framework. – 4. Human Rights Framework.– 5. Looking Forward.

1. Introduction

There is currently no federal legislation in Canada that explicitly regulates the collection or use of facial recognition technology or biometric data more generally. A single province, Quebec, brought into force the *Act to establish a legal framework for information technology* in 2001.¹ This often-overlooked legislation permits the use of facial recognition technology but imposes registration and reporting requirements when biometric data or systems are used for identification or authentication purposes.

Throughout the rest of Canada, the use of facial recognition technology is merely constrained by federal privacy laws that limit the collection, use and sharing of personal information. The Supreme Court of Canada has not yet considered the question of whether the use of facial recognition technology by state agencies engages a person's right to privacy under the *Charter of Rights and Freedoms*, and the relevant case law points in opposing directions. Given the lack of clear legal limits, Canadians are fortunate that there has been limited use of facial recognition technology in public settings.

The following paper sets out the relevant legal frameworks and summarizes the

reported uses of facial recognition technology in public spaces within Canada. It begins with a discussion of the private sector privacy framework and two investigations into the use of real-time facial recognition technology on unsuspecting shoppers. Next, it details the public sector privacy framework and the collection and use of biometric facial records at Canada's borders, including the "Faces on the Move" pilot project. Finally, it sets out the debate over whether the use of facial recognition technology in public would amount to a protected search under the *Charter*. The paper concludes with a brief look towards the future of Canadian privacy and AI legislation.

2. Private Sector Privacy Framework

Across most of Canada, the *Personal Information Protection and Electronic Documents Act (PIPEDA)* regulates the collection, use, and disclosure of personal information during commercial activity, including commercial surveillance.² Businesses operating in Quebec, Alberta, and British Columbia are subject to provincial laws that are substantially similar to PIPEDA and, as such, this section focuses only on the federal legislation.

Under PIPEDA, an individual's knowledge

* Article submitted to double-blind peer review.

¹ Quebec, *Act to establish a legal framework for information technology*, CQLR c C-1.1.

² Canada, *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (PIPEDA).

Leah West

and consent are required to collect, use, or share their personal information, and only for purposes that a reasonable person would consider appropriate in the circumstances.³ Personal information is defined in the legislation as information about an identifiable individual.⁴

There are exceptions to the consent requirement, such as when the information is “publicly available”.⁵ The phrase “publicly available” is defined in regulation and limited to information in a public telephone directory, public business directory, other statutorily mandated directories, and records relating to judicial or quasi-judicial proceedings. Personal information in a publication, such as a magazine, newspaper, or book, is also considered publicly available so long as the individual themselves provides that information to the publisher.⁶ Neither a photograph of someone in a public space nor a photograph posted on a social media platform constitutes publicly available information under PIPEDA.⁷

There have been two decisions by privacy regulators related to the public deployment of facial recognition technology by private actors in Canada. The first investigation, published in October 2020, examined the use of “Anonymous Video Analytics” technology implanted into directories in twelve malls owned by the Cadillac Fairview Corporation across Canada. Cameras were embedded into the directory and took temporary images of the faces of anyone within their field of view. Facial recognition software was then used to assess the age and gender of mall goers to gather demographic information and measure foot traffic. A unique identifier number was also assigned to each captured face.⁸ In their joint findings, the Privacy commissioners of Canada, Alberta and British Columbia agreed that the captured images, the numerical number assigned to each face and the assessment of age and gender all constituted personal information collected without valid

notice or consent.⁹

In reaching this conclusion, they found that facial images and biometric representations of those images were not only private information but that

biometric information sensitive in almost all circumstances. It is intrinsically, and in most instances permanently, linked to the individual. It is distinctive, stable over time, difficult to change and largely unique to the individual. Within the category of biometric information, there are degrees of sensitivity. Facial biometric information is more sensitive since possession of a facial recognition template can allow for identification of an individual through comparison against a vast array of images readily available on the internet or via surreptitious surveillance.¹⁰

This interpretation of the private nature of facial biometric information was reinforced in a subsequent investigation of Clearview AI’s facial recognition technology in 2021.¹¹

The second investigation, carried out by Office of the Information & Privacy Commissioner for British Columbia in 2023 examined the use of facial recognition software by four Canadian Tire stores in the province.¹² Over the course of three years, the stores created biometric templates of every person entering their store and compared them to templates of “persons of interest” for the stated purpose of loss prevention and staff and customer safety. If there was a match between a new customer and a person of interest, store management and security staff received an alert, a copy of the current image, prior images, and details of previously linked incidents. The match was then verified in person and the subject would either be surveilled or escorted from the property. The Commissioner found that the stores did not provide proper notice of this practice, nor did they receive consent to collect personal information. Relying on the findings from the aforementioned federal investigations, the Commissioner concluded “that the type of personal information at issue in this case reaches the highest level of sensitivity.”¹³

³ PIPEDA, Schedule 1.

⁴ PIPEDA, s. 2.

⁵ PIPEDA, s. 7.

⁶ Canada, *Regulations Specifying Publicly Available Information*, SOR/2001-7 (13 December 2000).

⁷ Canada, *Office of the Privacy Commissioner*, PIPEDA Findings #2021-001, at para 45 (OPC Clearview AI Investigation).

⁸ Canada, *Officer of the Privacy Commissioner*, PIPEDA Findings #2020-004, at para 43 (OPC Cadillac Fairview Investigation).

⁹ OPC Cadillac Fairview Investigation, para. 74.

¹⁰ OPC Cadillac Fairview Investigation, para. 79.

¹¹ OPC Clearview AI Investigation, para. 41.

¹² British Columbia, *Officer of the Information and Privacy Commissioner for British Columbia*, 2023 BCIPC 17 (BCIPC Canadian Tire Investigation).

¹³ BCIPC Canadian Tire Investigation, 18.

3. Public Sector Privacy Framework

The collection, use and disclosure of personal information within the federal government is governed by the *Privacy Act*.¹⁴ Like PIPEDA, the *Privacy Act* defines personal information as “information about an identifiable individual that is recorded in any form” but then provides an open list of examples including fingerprints, as well as information relating to a person’s race, age and ethnicity.¹⁵

Section 4 of the *Privacy Act* is fundamental. It states that “no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.”¹⁶ Subsequent provisions specify that where personal information is collected, the institution must, wherever possible, collect it directly from the individual and inform them of its purpose. An exception to these requirements arises if compliance might “defeat the purpose of prejudice the use for which the information is collected.”¹⁷

When it comes to sharing collected information, the starting point is that the government may not share personal information between government bodies without an individual’s consent. However, again there are exceptions to the consent requirement, several which apply in the national security context. For example, personal information may be disclosed “for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose.”¹⁸ This means that information collected by the Royal Canadian Mounted Police (RCMP) in furtherance of its duties to preserve peace, prevent crime and enforce the law under s. 18 of the *RCMP Act* may be disclosed to other federal, provincial or municipal law enforcement agencies. Personal information may also be released by government agencies to a specified investigative body for law enforcement or a lawful investigation, or under a federal-provincial or international agreement used for law enforcement or lawful investigation.¹⁹

Another exception is that personal

information may be disclosed without consent when authorized by other federal legislation, including the *Security of Canada Information Disclosure Act (SCIDA)*. Section 5 of SCIDA permits a government agency to disclose information to Canada’s national security and intelligence institutions “where the disclosure will contribute to the exercise of the recipient institution’s jurisdiction, or the carrying out of its responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada; and the disclosure will not affect any person’s privacy interest more than is reasonably necessary in the circumstances.”²⁰ Importantly, information collected at Canada’s borders may be shared with other agencies via SCIDA. It is here where Canada has seen the greatest implementation of facial recognition technology by federal agencies.

Canadians and travelers are subject to strict oversight and monitoring at Canada’s border crossings and airports, primarily by officers from the Canada Border Services Agency (CBSA). Upon arrival in Canada, s. 11(1) of the *Customs Act* stipulates that everyone must present themselves to an officer without delay and truthfully answer any questions asked by the officer in the performance of his or her duties under any act of parliament.²¹ In 2017, Primary Inspection Kiosks (PIKs) were introduced in ten Canadian airports. These kiosks validate ePassports and use facial recognition technology to confirm arriving passengers match the presented travel document.²² CBSA relies on s. 11 to collect this information, as well as s. 18(1) of the *Immigration and Refugee Protection Act (IRPA)* which require every person seeking to enter and remain in Canada to present themselves for examination by an officer.

Under IRPA, non-citizens applying to live and work, make a refugee claim, or gain permanent residence status in Canada must also answer all questions put to them truthfully and produce all relevant documents and evidence requested by an officer.²³ Since

¹⁴ Canada, *Privacy Act*, RSC, 1985, c. P-2.

¹⁵ *Privacy Act*, s 2.

¹⁶ *Privacy Act*, s 4.

¹⁷ *Privacy Act*, s 5(3)(b)

¹⁸ *Privacy Act*, s 8(2)(a).

¹⁹ *Privacy Act*, s 8(2)(e)-(f).

²⁰ Canada, *Security of Canada Information Disclosure Act*, SC 2015, c 20, s.2, s 5.

²¹ Canada, *Customs Act*, RSC 1985, c. 1 (2nd Supp), s 11.

²² Canada, *National Security and Intelligence Review Agency, Study of the Government of Canada’s Use of Biometrics in the Border Continuum*, 2022, 51 (NSIRA).

²³ Canada, *Immigration Refugee Protection Act*, SC 2001, c 27, s 16(1) (IRPA).

Leah West

2018, this includes the provision of biometric data by all applicants, other than US citizens, making a refugee claim or applying for a visa or permanent residence.²⁴ Currently, regulations made under IRPA limit the collection of biometric data to fingerprints.²⁵ This, however, is not specified in the legislation and could be expanded to include the creation of facial biometric templates using photographs already required with all applications. Once collected by immigration officials, fingerprints are shared with the RCMP, which compares them against records of criminals, deportees and other applicants and claimants. If there is a potential match, the RCMP may disclose those fingerprints along with a person's name, known aliases, date of birth, and gender, within the RCMP and to other law enforcement agencies to establish or verify the identity of a person to prevent, investigate or prosecute any federal or provincial offence.²⁶

Immigration Refugee and Citizenship Canada (IRCC) also collects and shares biometric information collected through the Passport Program with law enforcement and other national security agencies.²⁷ Anyone applying for a Canadian travel document must submit two photographs that are digitized and transferred into the "Facial Recognition Solution" (FRS), which converts the images into a biometric template.²⁸ That template is then used to match the photo against the individual's previous applications as well as existing templates from all previous applications (approximately 55 million as of 2020) to ensure they are not on an existing watchlist.²⁹ Other security agencies will often make a request for information from IRCC pursuant to their authorities and s. 4 of the *Privacy Act*, and the requested information is shared by IRCC under s. 5 of *SCIDA*. In practice, the other agency provides a photograph of a person of interest to IRCC who then converts it into a biometric template and runs it through the FRS to confirm their identity.³⁰

Aside from the PIK's at ports of entry, the

only known deployment of facial recognition technology in a public setting by a federal agency to date was the "Faces on the Move" pilot project.³¹ This project, run by CBSA, involved the live capture of facial images of travelers passing through Terminal 3 of the Toronto Pearson International Airport between June and November 2016. Those images were checked in real time against two databases. The first, a control list consisting of the images of 65 CBSA volunteers, and the second, an operational watchlist with images of 4,860 previously deported individuals.³² Prior to the project, CBSA consulted with the Federal Privacy Commissioner to complete the required Privacy Impact Assessment (PIA), which is mandated by a policy directive issued by the Treasury Board of Canada.³³ A PIA is a policy process that must be undertaken by any government institution that uses or intends to use personal information, or when there is a substantial change to any such program.³⁴

CBSA's assessment led to changes to the project, namely the decision not to use watchlists from other government agencies and dropping plans to share information with law enforcement agencies if a previously deported person was identified but not intercepted before leaving the airport.³⁵

Faces on the Move was studied as part of a larger review into Canada's use of biometrics at its borders by the National Security Intelligence Review Agency (NSIRA) published in July 2022. In its report, NSIRA found that the legal authority relied upon by CBSA for the collection of live capture images, sections 15-18 of IRPA, was concerning. NSIRA found that the use of real-time facial recognition was not consistent with those provisions which "presume an overt interaction between the traveler and CBSA officials, and the knowing presentation by

³¹ NSIRA, 22.

³² NSIRA, 22.

³³ Canada, *Canada Border Services Agency, Archived - Faces on the Move: Multi-camera screening, Privacy Impact Assessment (PIA) Executive Summary*, 2016, online: www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-airp/fotm-eng.html. Privacy Impact Assessments are required under the Treasury Board of Canada Secretariat Directive on Privacy Practices for any federal program that may have an impact on the personal information of individuals.

³⁴ Treasury Board of Canada, *Directive on Privacy Practices* (effective 9 October 2024), www.tbssct.canada.ca/pol/doc-eng.aspx?id=18309#appC.

³⁵ NSIRA, 23.

²⁴ IRPA, s 10.1.

²⁵ NSIRA, 31-32.

²⁶ IRPA, s 150; Immigration and Refugee Protection Regulations, SOR/2002-227, s 13.11.

²⁷ NSIRA, 46.

²⁸ NSIRA, 43.

²⁹ NSIRA, 43-44.

³⁰ NSIRA, 47.

travelers of their individual documents, fingerprints and photographs during their examination.”³⁶ NSIRA was not satisfied the CBSA had “clear authority for the collection of travelers’ facial biometrics, particularly prior to – and away from – the point of formal examination.”³⁷

Outside of the border continuum, law enforcement agencies in Canada are using facial recognition software to identify images of suspects, victims and potential witnesses.³⁸ The most controversial instance of this practice was the RCMP’s use of Clearview AI’s software, which was subject to an investigation by the federal Privacy Commissioner in 2023.³⁹ In his report, the Commissioner found the RCMP violated s. 4 of the *Privacy Act* because they failed to confirm that Clearview’s practices were consistent with PIPEDA. (In a separate investigation the Commissioner found that Clearview had not obtained the requisite consent and used collected images and information for inappropriate purposes.⁴⁰) In his view, a law enforcement activity cannot be legally compliant with privacy legislation if that activity is dependent on a tool that breaches Canadian privacy legislation.

In response to the Commissioner’s findings and public pressure, the RCMP established a National Technology Onboarding Program (NTOP) “to ensure the responsible use of operational technologies by the RCMP and encourage more public transparency of those technologies.”⁴¹ The NTOP is responsible for conducting assessments and evaluations of new and existing operational technologies to ensure that they meet an operational need. The program reports that “technologies that are privacy intrusive or contain artificial intelligence are given the highest priority.”⁴²

³⁶ NSIRA, 25.

³⁷ NSIRA, 25.

³⁸ Privacy and Access Council of Canada, *Facial Recognition Use by Law Enforcement in Canada: Realities, Reservations, and Recommendations*, 2021, 3.

³⁹ Canada, *Office of the Privacy Commissioner*, *Police use of Facial Recognition Technology in Canada and the way forward*, 2023.

⁴⁰ OPC Clearview AI Investigation.

⁴¹ RCMP, *National Technology Onboarding Program*, 19 March 2025, online: <https://rcmp.ca/en/specialized-policing-services/technical-operations/national-technology-onboarding-program>.

⁴² RCMP, *National Technology Onboarding Program, Transparency Blueprint: Snapshot of operational technologies*, 16 July 2024, <https://rcmp.ca/sites/default/files/doc/national-technology-onboarding-program-transparency-blueprint.pdf>, 5.

In its only public report to date, the NTOP explained that, at that time, the RCMP uses facial recognition technology solely for face matching to process, sort, and analyze large volumes of images and videos, and only to process evidence obtained lawfully during the course of an investigation.⁴³ (Of course, huge volumes of video evidence may be lawfully collected from private persons and entities, public security cameras, police body cam footage etc., without a warrant, so this is not necessarily a significant limiting factor). The report also anticipated that the RCMP would deploy the technology in the future to identify victims and suspects. No policy or technical details were provided.

In fact, the only police force in Canada that currently has a public policy on the use of Artificial Technology is the Toronto Police Service.⁴⁴ To date, TPS is only using facial recognition technology to match images against a database of mug shots and all potential matches are reviewed by one of two trained facial recognition analysts on the force.⁴⁵

4. Human Rights Framework

It is unclear whether the use of facial recognition technology by a state agency like the RCMP or CBSA would constitute an unreasonable infringement upon a person’s right to privacy guaranteed by section 8 of the *Charter of Rights and Freedoms*.

Section 8 guarantees the right to be secure against unreasonable search or seizure. This has been interpreted to mean that the *Charter*’s protections are only triggered when there is a search or a seizure that is subject to “reasonable expectation of privacy” (REP).⁴⁶ For example, one cannot reasonably claim a privacy interest in the collection of their name, the address of their workplace, or their hair colour. Rather, personal information attracting constitutional protection is “information which tends to reveal intimate details of the lifestyle and personal choices of the

⁴³ *Ibid.*, 20

⁴⁴ Toronto Police Services Board, *Use of Artificial Intelligence Technology*, policy amended 11 January 2024, <https://tpsb.ca/policies-by-laws/board-policies/19-5-use-of-artificial-intelligence-technology>.

⁴⁵ Toronto Police Services, *Artificial Intelligence*, accessed 3 June 2025, online: www.tps.ca/police-reform/artificial-intelligence/#:~:text=The%20system%20uses%20a%20fixed,the%20investigator%20for%20additional%20review.

⁴⁶ *R v S.A.B.*, 2003 SCC 60 at para. 38.

Leah West

individual.”⁴⁷

Once triggered, a government search or seizure must be “reasonable” to not fall afoul of the *Charter*. A search is presumptively unreasonable if it is not pre-authorized by a neutral and impartial arbiter capable of acting judicially.⁴⁸ This is typically understood as a need to obtain a judicially authorized warrant. Alternatively, a warrantless search may be reasonable if it satisfies three criteria: (1) the search is authorized by law; (2) the law itself is reasonable; and (3) the search is carried out in a reasonable manner.⁴⁹

The existence of a REP requires a contextual assessment – the “totality of the circumstances” under which the alleged search takes place.⁵⁰ The factors considered in this assessment are: (1) the subject matter of the alleged search; (2) the individual’s interest in the subject matter; (3) the individuals subjective expectation of privacy in the subject matter, and (4) whether that subjective expectation is objectively reasonable given the totality of the circumstances.⁵¹ This means where the search takes place, whether the subject matter of the search was in public view, and whether the information was already in the hands of third parties are all relevant to the question of REP.⁵²

For instance, a person generally does not have a REP as they move through public spaces, drive down public roads, or shop in public stores. Lower courts have repeatedly found that surreptitiously recording people in public places, including the area immediately outside their homes, is not a search under s 8.⁵³ However, in cases involving online activity, the Supreme Court of Canada has recognized that s 8 of the *Charter* protects anonymity in public places as a feature of privacy.⁵⁴ This is because “[a]nonymity permits individuals to act in public places but to preserve freedom from identification and surveillance.”⁵⁵ By simply appearing in public “an individual does not automatically forfeit his or her interest in retaining control over the

personal information which is thereby exposed.”⁵⁶ Thus, it is likely that whether the use of FRT by a state agency engages a person’s s 8 rights will depend on what other information is gleaned from a positive identification and whether it reveals anything about their lifestyle, personal choices, or core biographical data.

Importantly, however, the Supreme Court has also found that persons have a diminished expectation of privacy at the border.⁵⁷ In *R v Simmons*, the Supreme Court considered the constitutionality of a strip search conducted by a customs officer at an airport who had reasons to suspect that the accused was secreting narcotics. The Court reasoned:

People do not expect to be able to cross international borders free from scrutiny. It is commonly accepted that sovereign states have the right to control both who and what enters their boundaries. For the general welfare of the nation the state is expected to perform this role. Without the ability to establish that all persons who seek to cross its borders and their goods are legally entitled to enter the country, the state would be precluded from performing this crucially important function. Consequently, travelers seeking to cross national boundaries fully expect to be subject to a screening process.⁵⁸

The Supreme Court went on to find that “routine questioning,” luggage searches, and frisk and pat down searches conducted by customs officers without any individualized suspicion were not unreasonable searches under section 8 of the *Charter*.⁵⁹ Thus, it is likely that use of facial recognition technology at ports of entry, like that used in the Faces on The Move project would be consistent with the Charter.

5. Looking Forward

Numerous bodies have recommended that amendments are needed to Canada’s privacy legislation to create explicit requirements around the collection, sharing and use of biometric data in both the public and private sector. In November 2022, the Liberal

⁴⁷ *R v Plant*, [1993] 3 SCR 281 at 293.

⁴⁸ *Hunter et al. v Southam Inc.*, [1984] 2 SCR 145.

⁴⁹ *R v Collins*, [1987] 1 SCR 265 at para. 23.

⁵⁰ *R v M (MR)*, [1998] 3 SCR 393 at 286.

⁵¹ *R v Spencer*, 2014 SCC 43 at para. 18 [Spencer]

⁵² *R v Tessling*, 2004 SCC 67 at para. 32.

⁵³ See *R v Hoang*, 2021 ONSC 6054; *R v Aubrey*, 2022 ONSC 635; *R v Ngo*, 2022 ONSC 3700; *R v Kawal*, 2022 ONCJ 475.

⁵⁴ *Spencer*, paras. 7-12.

⁵⁵ *Spencer*, para. 40.

⁵⁶ *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, para. 27.

⁵⁷ *R v Simmons*, [1988] 2 SCR 495, at para. 4 [Simmons].

⁵⁸ *Simmons*, at para. 49.

⁵⁹ *Simmons*, at para. 50.

Government tabled Bill C-27 the *Digital Charter Implementation Act, 2022* that, if passed, would create three significant new pieces of legislation: the Consumer Privacy Protection Act (a modernized PIPEDA), the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act (AIDA).⁶⁰ Regrettably, the Bill failed to address the issue of biometric collection, let alone the privacy implications of facial recognition technology. Moreover, AIDA did not control or limit AI use but rather sets out reporting and mitigation requirements for private developers of “high impact” system (a term to be later defined in regulations). Ultimately, the bill died on the order paper when Parliament was dissolved in early 2025. There was remarkably very little discussion of AI and even less of privacy during the federal election campaign, and the new government under Prime Minister Mark Carney has, at the time of writing, not made it a priority.

⁶⁰ Canada, House of Commons (44th, 1st) 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.

