ACCESS TO JUSTICE IN DATA PRIVACY: ADDRESSING SYSTEMIC BARRIERS TO PRIVACY PROTECTION IN CANADIAN LAW

ADAM RICHERT

THOMPSON RIVERS UNIVERSITY – FACULTY OF LAW

ABSTRACT

Most Canadians do not understand their privacy rights or know how to defend them when their personal information is misused. This paper argues that Canada's privacy protections are inadequate and fragmented, leaving citizens without consistent safeguards or meaningful remedies. The legal framework is split between federal and provincial jurisdictions, creating gaps and inconsistencies. Provincial courts have developed different approaches to privacy torts, and the Office of the Privacy Commissioner lacks real enforcement power. This paper examines key cases involving biometric data collection, workplace surveillance, and data breaches to show how current laws struggle to protect Canadians. Recent legislative reform efforts, particularly Bills C-26, C-27, and C-63, died in Parliament in 2025 without becoming law, leaving the outdated PIPEDA framework unchanged. The paper proposes three concrete reforms: establishing a single federal privacy standard across all provinces and industries, creating a statutory tort for privacy violations, and strengthening substantive privacy rights to match international standards like the EU's GDPR. These changes are necessary to give Canadians real access to justice and to treat privacy as the fundamental right it should be.

Table of Contents

ACCESS TO JUSTICE IN DATA PRIVACY: ADDRESSING SYSTEMIC BARRIERS TO PRIVACY PROTECTION IN CANADIAN LAW 4

Introduction 4

Legal Framework for Data Privacy 5

A. Supreme Court of Canada Jurisprudence 6

B. Federal and Provincial Privacy Legislation 6

Barriers to Accessing Data Privacy Protections 8

A. Concerns with biometric data collection 8

It is a justiciable issue 9

Required consent is still a grey area 10

B. The imbalance of the common law in privacy claims 12

Intrusion upon seclusion 12

The British Columbia Privacy Act 13

Key differences and what that means for Canadians 14

C. Limited applications of PIPEDA and the Office of the Privacy Commissioner 15

Legal Reforms and Policy Recommendations 17

A. Setting a federal standard for privacy rights 17

B. Creating a standardized tort to defend privacy rights 18

C. Strengthening privacy rights 19

Conclusion 20

References 21

ACCESS TO JUSTICE IN DATA PRIVACY: ADDRESSING SYSTEMIC BARRIERS TO PRIVACY PROTECTION IN CANADIAN LAW

Introduction

As Canadian industries have become more reliant on technology, the privacy rights of employees have become a rising topic of discussion. The current Privacy Commissioner of Canada Phillipe Dufresne was recently quoted, saying "Privacy is a fundamental right because personal information is a core part of who we are as individuals, and respecting privacy rights is essential to our dignity and to the enjoyment of other fundamental freedoms."[1] Unfortunately, Canada has fallen behind when protecting people's privacy rights.

Canada worked to pass three separate bills concerning technology and privacy rights including Bill C-26, Bill C-63, and Bill C-27.[2] However, all three bills died on the Order Paper when Parliament was prorogued on January 6, 2025. Of these, only Bill C-26 has been revived. The new government reintroduced it as Bill C-8 in June 2025, which would require businesses operating critical infrastructure to adhere to specific cybersecurity procedures overseen by the Minister of Industry.[3] Bill C-63 aimed to protect Canadians online from "harmful content" but remains dead with no indication it will be reintroduced.[4] Bill C-27's

[1] Aaron Shull, "Safeguarding Privacy and Preserving Freedom of Thought in Canada: A Call to Action", *Centre for International Governance Innovation,* (March 28, 2024). (https://www.cigionline.org/articles/safeguarding-privacy-and-preserving-freedom-of-thought-in-canada-a-call-to-action/).

[2] Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 44th Parl, 2022 (first reading 14 June 2022); Bill C-63, *An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide Internet service and to make consequential and related amendments to other Acts*, 1st Sess, 44th Parl, 2024 (first reading 26 February 2024); 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, 44th Parl, 2022 (first reading 16 June 2022).

[3] Blakes, "Digital Policy Issues Face Uncertain Future After Prorogation of Parliament" (26 January 2025), online: Blakes https://www.blakes.com/insights/digital-policy-issues-face-uncertain-future-after-prorogation-of-parliament/; Data Guidance, "Canada: Bill C-27 dies after Parliament is prorogued" (12 February 2025), online: Data Guidance; Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, 1st Sess, 45th Parl, 2025 (first reading 18 June 2025); Gowling WLG, "Critical infrastructure cyber security bill" (19 June 2025), online: Gowling WLG https://gowlingwlg.com/en-ca/insights-resources/articles/2025/critical-infrastructure-cyber-security-bill.

[4] Tech Policy Press, "Canada's Online Harms Bill is Dead (Again)" (29 April 2025), online: Tech Policy Press https://techpolicy.press/canadas-online-harms-bill-is-dead-again-three-questions-to-consider-for-the-next-round; Gowling WLG, "Privacy and cyber bills: What to expect post-election" (24 April 2025), online: Gowling WLG

intention was to implement a digital charter protecting Canadians' privacy rights through the proposed Consumer Privacy Protection Act, Personal Information and Data Protection Tribunal Act, and Artificial Intelligence and Data Act.[5] It also remains dead, leaving Canada's outdated privacy framework under PIPEDA unchanged.[6] This follows the implementation of the European Union's ("EU") 2018 EU General Data Protection Regulation ("*GDPR*").[7] Because of the government's prorogation, none of these bills have been made into law, leaving many Canadians in the dark with fossilized protections not equipped to deal with modern issues.

Privacy rights are exceptionally fundamental in employment law, yet many workers face systemic violations. Canadian privacy laws are designed to protect personal data, but many Canadians remain vulnerable to employer surveillance, data exploitation, and limited access to justice. The existing legal framework fails to address the unique vulnerabilities of these workers. Legal loopholes allow employers to collect, store, and use personal data with minimal oversight or consequences. Many Canadians do not know their privacy rights in the workplace, and even if they do, they are unsure how to defend them.

This paper examines the legal gaps in privacy protections, reviews relevant precedents, and proposes reforms to ensure more substantial digital rights for Canadians.

Legal Framework for Data Privacy

Canada is trying to enact new legislation to reflect modern privacy issues. However, Bills C-26, C-27, and C-63 are not yet law,[8] and Canadians are left with outdated laws. With the rapid advancement and reliance on technology, these older laws do not protect the

---

https://gowlingwlg.com/en-ca/insights-resources/articles/2025/privacy-and-cyber-bills-what-to-expect-post-election.

[5] Canada, Library of Parliament, "Legislative Summary of 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*" (Publication No 44-1-C27-E, 2022).

[6] Gowling WLG, "Federal privacy reform: Where we left off and what's next" (25 September 2025), online: Gowling WLG https://gowlingwlg.com/en-ca/insights-resources/articles/2025/federal-privacy-reform.

[7] Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119, 1

[8] See notes 1,2 and 3.

Canadians they intend to. This section will review relevant federal and provincial legislation as to how those laws leave gaps in privacy law.

A. Supreme Court of Canada Jurisprudence

The Supreme Court of Canada ("SCC") opened the modern door for workplace privacy rights with *R v Cole* ("*Cole*") in 2012. The SCC in *Cole* stated that people have a reasonable expectation of privacy regarding their work laptops.[9] This decision triggered a discussion of workplace privacy rights regarding technology. In obiter, the SCC left the door open regarding the finer points of routine workplace inspections.[10] However, it is clear that there is a precedent that employers who give technology to employees do not give them the right to arbitrarily search for that technology. Since this decision, legislators have tried to fill the gaps the SCC left open.

B. Federal and Provincial Privacy Legislation

Two central federal legislations oversee the privacy of Canadians – *PIPEDA* and the *Privacy Act*. *PIPEDA* was enacted in 2004. *PIPEDA* oversees what businesses can do with people's private information, gives guidelines for these businesses to follow, and gives the minister of privacy the ability to investigate complaints against companies reported for breaking these regulations.[11] While Canada's *PIPEDA* establishes broad privacy protections, its application to precarious workers is unclear and insufficient. *PIPEDA* does not govern how private-sector organizations handle personal data and lacks explicit provisions addressing data privacy in employment relationships outside of those under the federal government.[12]

---

[9] *R. v Cole*, 2012 SCC 53, at para 54, [*Cole*].
[10] *Cole* at para 60.
[11] Office of the Privacy Commissioner of Canada "Personal Information Protection and Electronic Documents Act (PIPEDA) – Overview" *Privacy Laws in Canada* Government of Canada, (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/).
[12] Office of the Privacy Commissioner of Canada "PIPEDA: A Brief Overview" *Privacy Laws in Canada* Government of Canada (https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/).

The second piece of federal legislation is the *Privacy Act.* The *Privacy Act* was first enacted in 1983.[13] The *Privacy Act* sets out Canadians' privacy rights with the federal government.[14] The federal government stores information in various "information banks." Different legislative bodies have access to different information banks, but some, such as CSIS, can access any bank if they can cite special circumstances like national security.[15] People can request to see what information is stored at a federal institution. The institution reveals what bank that information is stored under but not what other institutions have access to it.[16] It must be stressed that both *PIPEDA* and the *Privacy Act* apply only to federally regulated organizations. In many Canadian provinces, there is no omnibus legislation overseeing privacy rights. However, British Columbia is one of three provinces that has its own privacy legislation.

In British Columbia, the Personal Information Protection Act ("*PIPA*") balances people's rights to privacy with the need for organizations to collect information.[17] A key theme from this piece of legislation that will come up later in this paper is the concept of "balancing privacy rights with the legitimate interests of the company." Many privacy law cases in British Columbia are boiled down to this. This concept is not explicitly written in *PIPA* but adopted under it from older guidelines of the Office of the Privacy Commissioner.[18]

When it comes to employment law, the primary legislation is the federal *Employment Standards Act.* British Columbia has its own version of the act as well. These acts notably

---

[13] Department of Justice Canada "Modernization of the Privacy Act" *Justice Laws Website* Government of Canada (https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html#s1).
[14] Department of Justice Canada *Personal Information Protection and Electronic Documents Act (PIPEDA)* Government of Canada (https://laws-lois.justice.gc.ca/PDF/P-21.pdf).
[15] Canada Revenue Agency "Info Source – Appendix" *Canada.ca* Government of Canada (https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/access-information-privacy-canada-revenue-agency/info-source-appendix.html).
[16] Privacy Act (R.S.C, 1985, c P-21), ss 13(1)–16(1).
[17] Personal Information Protection Act (SBC 2003), c 63, s 2.
[18] McMillan LLP "OPC Takes Firm Stance on Privacy in the Workplace: Takeaways for Employers" *McMillan,* (https://mcmillan.ca/insights/publications/opc-takes-firm-stance-on-privacy-in-the-workplace-takeaways-for-employers/).

"promote the fair treatment of employees and employers, encourage open communication between employers and employees, and provide fair and efficient procedures for resolving disputes."[19] Albeit, neither the federal nor BC legislation contains regulations governing privacy standards in the workplace.

Despite all this legislation, many do not know what laws directly affect them. In British Columbia, *PIPA* protects everyone, but as we will see, the extent of *PIPA*'s protections can be quite limited. Many trained professionals struggle to interpret where to draw the line. Consider the average person—many have little knowledge of their rights, and if those rights are violated, they often do not know how to fight for them. In the next section, this paper will discuss the current barriers Canadians face when trying to access privacy protections.

Barriers to Accessing Data Privacy Protections

This section will focus on three areas that demonstrate the growing issues in Canada. First, advancements in biometric data collection have led courts to inconsistent findings, which blurs the line of privacy rights. Second, different provinces have separate pathways for individuals to defend their rights. Some provinces have created a new common law tort of intrusion upon seclusion, whereas others, like British Columbia, use statutory torts. Third, this paper will discuss changes the Office of the Privacy Commissioner made to their guidelines for workplace privacy. It will then go into how these guidelines are widely ignored in the private sector and has been inconsequential for most Canadians.

A. Concerns with biometric data collection

The first growing concern is the use of biometric data collection. Many organizations now require employees to have fingerprints or even facial recognition technology for various reasons. This leaves Canadians with many questions: Are organizations allowed to do this

[19] Employment Standards Act [RSBC 1996], c 113, ss 2(b)–(d).

without consent? What justification does an organization require to request this collection? And is this even a justiciable issue? This section will discuss three cases that outline where Canada stands so far and what questions remain.

It is a justiciable issue

In January of 2024, the British Columbia Court of Appeal ("BCCA") ruled that Google's collection of biometric data of non-google users was a justiciable issue.[20] In October 2015, Google introduced Face-grouping for Android phone users.[21] Face-grouping was a facial recognition AI that would analyze photos taken by Android phones and create albums of photos throughout the phone of the same people. The plaintiff saw this as a privacy violation when taking photos of his children or his non-Android using friends.[22] He understood that, as the user, he likely consented to this software through a boilerplate contract in an update. However, he knew his friends and children could not have consented to being used in this software.[23] He filed a class action for those who could not consent and were subject to this AI.[24] The BCCA ultimately stated that he did have a cause of action under the *Privacy Act*.[25] This case has been remitted to the BC Supreme Court to see if the now actionable claim violates individual privacy rights.

This case demonstrates two main points. First, the BCCA seems to adopt the notion that biometric data is "intrinsically private in the same way as fingerprints or DNA."[26] Second, the collection of this information without consent is an actionable issue. With this case still being decided in BC courts, we can see similar actions being taken in Ontario.

[20] *Situmorang v Google*, LLC, 2024 BCCA 9 at para 95, [*Situmorang*].
[21] *Situmorang* at para 1.
[22] *Situmorang* at para 6.
[23] *Situmorang* at para 9.
[24] *Situmorang* at paras 9 and 10.
[25] *Situmorang* at para 85.
[26] *Situmorang* at paras 33 and 63.

Required consent is still a grey area

During the COVID-19 pandemic, McMaster University began using proctored online exams through the Respondus system.[27] Respondus limited online access to students' computers but also had a biometric recognition AI that could access students' cameras and microphones on their computers.[28] It would monitor and record the students for the entirety of their exams to recognize cheating body language.[29] Students had little choice but to accept the conditions set by the university, which stated that the university "retains complete autonomy, authority, and discretion to employ proctored online exams, prioritizing administrative efficiency and commercial viability, ***irrespective of necessity.***"[30]

One student filed a complaint with the Office of the Information and Privacy Commissioner of Ontario, which investigated. They ultimately decided that McMaster University had a legitimate, lawful interest in using the proctored exam.[31] However, they did not correctly inform students of the data collection, nor did they understand that the Respondus system used the recordings of students to improve their own software.[32] Ultimately, McMaster University was not held liable, and the privacy commissioner's jurisdiction restricted any recommendation toward the proctoring company itself.[33]

This is a concerning outcome. The decision recognized that if the collection of information is lawful, consent is not obligatory. It also highlighted the limits of privacy laws on private companies. Students in this situation were forced into the collection of their information without their consent if they wanted to pursue their education. What is more

[27] *Privacy Complaint PI21-00001; McMaster University (Re)*, [2024] OIPC No 39 at para 1, [*McMaster*].
[28] *McMaster* at paras 4-7.
[29] *McMaster* at paras 58 and 62.
[30] *McMaster* at para 63.
[31] *McMaster* at para 166.
[32] *McMaster* at para 77-89.
[33] *McMaster* at para 160.

confusing is that this line of reasoning is in direct contrast with a recent BC privacy commissioner decision.

In April of 2023, the BC Privacy Commissioner wrote a fiery investigation report on the use of facial recognition technology in retail stores. Canadian Tire was using a program called FaceFirst in certain locations.[34] FaceFirst is an AI that examined security camera footage and used facial recognition software to flag potential shoplifters against their internal persons of interest database.[35] Still images of every customer's face were kept in the system for 30-60 days, and if no match was found, they were deleted.[36] If an image was flagged as a "person of interest", it would be kept in the database until it was manually deleted.[37] The Privacy Commissioner used *PIPA* to demonstrate that consent is required for this type of personal information collection, and this situation did not condone an exception.[38]

This complaint demonstrates a much stricter approach to privacy rights. Ontario and British Columbia have different legislation that regulate their privacy, but having different laws should not demonstrate such opposite findings. In Ontario, the privacy commissioner has much less oversight over private companies like Canadian Tire. With the Ontario Privacy Commissioner's reasoning of "in the lawful interests of the company", it would also be more likely to condone the collection of biometric information in retail. Canadians should know what their privacy rights are, which should not vary drastically depending on the province in which they live. These issues are at least justiciable, but there is no consistency of where triers of fact will land on these issues, and that should be a concern for Canadians.

Even if legislators sort out Canadians' privacy rights, many still don't know how Canadians can defend them. Earlier, I outlined how people can request investigations from

[34] Investigation Report 23-02; Canadian Tire Associate Dealers' use of facial recognition technology (Re), [2023] BCIPCD No 17 at para 20, [*Canadian Tire*].
[35] *Canadian Tire* at para 48.
[36] *Canadian Tire* at paras 48-50.
[37] *Canadian Tire* at paras 51-56.
[38] *Canadian Tire* at para 57.

privacy commissioners, but even if they can investigate an issue, they are limited in what consequences they can give. Since there is no omnibus legislation, this leads many Canadians to resort to the common law, which also has its problems.

B. The imbalance of the common law in privacy claims

Canada has an issue regarding where to draw the line in privacy law. If Canada can define where to draw the line, there will still be an issue of how Canadians can defend what rights they have.

Intrusion upon seclusion

Earlier, this paper discussed the Situmorang case, in which the BCCA identified Google's privacy violation as an actionable issue under the BC *Privacy Act*.[39] As this case goes to trial, the BC courts will likely have to answer whether British Columbia will recognize the tort of intrusion upon seclusion. The Ontario Court of Appeal ("ONCA") recognized this new tort in the 2012 case *Jones v Tsige* ("Jones).[40]

ONCA defined intrusion upon seclusion as "one who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person."[41] ONCA outlined the elements required for the tort as: (1) the invasion must have been reckless or intentional, (2) the defendant invaded the plaintiff's information without lawful justification, and (3) a reasonable person would find the invasion to be highly offensive causing distress, humiliation or anguish.[42]

Ontario does not have a privacy act that mirrors *PIPA* or the *Privacy Act* in BC. Instead, it relies on the federal *PIPEDA* legislation, which again only affects those working

[39] See note 17.
[40] *Jones v. Tsige*, 2012 ONCA 32, [*Jones*].
[41] *Jones* at para 70.
[42] *Jones* at para 71.

under federal jurisdiction. This tort act is the only private law infringement of privacy rights in Ontario.

The British Columbia Privacy Act

British Columbia has not recognized the tort of intrusion upon seclusion because they have a statutory framework. The BC *Privacy Act* explicitly establishes its own tort for privacy violations.[43] The *Privacy Act's* definition of the tort states, "It is a tort, actionable without proof of damage, for a person, willfully and without a claim of right, to violate the privacy of another."[44] Recent case law demonstrates key differences between the common law tort in Ontario and the statutory tort in British Columbia.

Ari v Insurance Corporation of British Columbia outlines this difference best. In 2010, 78 individuals had their information stolen by an employee of ICBC. Their addresses, names and license plates were given to criminals who targeted the individuals with arson, theft and shootings.[45] This case was filed as a class action and has gone back and forth through the BC courts, with the most recent decision happening in August 2023. Throughout this back-and-forth, the British Columbia Supreme Court ("BCSC") and the BCCA have both given detailed overviews of the extent of the *Privacy Act* in BC and key differences between it and other common law forms of a similar tort.

In its 2023 decision, the BCCA outlined that the *Privacy Act* does not require a "consequence requirement."[46] As stated earlier, the tort of intrusion upon seclusion requires a reasonable person test to find the invasion "highly offensive." The *Privacy Act* states in a different fashion that the "nature and degree of privacy to which a person is entitled is that which is reasonable in the circumstances, giving due regard to the lawful interest of others,

[43] *Privacy Act* [RSBC 1996] chapter 373, [*Privacy Act*].
[44] *Privacy Act* at s 1.
[45] Parsons & Corrin LLP "ICBC Privacy Breach Class Action" *Parsons & Corrin* (https://parsonscorrin.ca/practice-areas/class-actions/icbc-privacy-breach-class-action/).
[46] *Insurance Corporation of British Columbia v. Ari*, 2023 BCCA 331 at para 105, [*Ari*].

the nature, incidence and occasion of the Act or conduct, and the relationship of the parties."[47] The BCCA used these differences to boast about the superiority of a statutory framework, but there are other key differences in the wording that raise problems for the statutory tort as well.[48]

Key differences and what that means for Canadians

Under the first stage, the tort of intrusion upon seclusion states that intrusion can be intentional ***or reckless***. The BC *Privacy Act* requires a willful intrusion.[49] The BCCA touched on this when they considered the hypothetical argument if the ICBC employee accidentally took the plaintiff's information.[50] When considering this in context with the Google facial recognition software, it will be more difficult to argue that the information was collected willfully than to say it was taken recklessly.

Another key difference is that the *Privacy Act* covers liability when there is a failure to act if there was an obligation to do so[51], or by acting with reckless indifference.[52] A recent pair of cases decided by the BCCA has confirmed that in British Columbia, database defendants (organizations that collect and store personal information about individuals) are subject to liability if they fail to respond appropriately to a third-party cyber-attack.[53]

These cases directly counter what ONCA has decided in the past under the intrusion upon seclusion tort.[54] The main difference seen here is that the common law tort requires an invasion of the privacy of the affected individual. In the context of third-party data breaches, the data defendant did not do anything to invade the person's privacy, so the claim failed.

---

[47] *Privacy Act* ss 1(2) and (3).
[48] *Ari* at para 107.
[49] *Privacy Act* at s 1.
[50] *Ari* at para 116.
[51] *Odhavji Estate v Woodhouse*, 2003 SCC 69 at para 23.
[52] *Peracomo Inc. v TELUS Communications Co.*, 2014 SCC 29 at para 57.
[53] See *Campbell v Capital One Financial Corporation*, 2024 BCCA 253 and *G.D. v South Coast British Columbia Transportation Authority*, 2024 BCCA 252.
[54] See *Owsianik v. Equifax Canada Co.*, 2022 ONCA 81, *Obodo v. Trans Union of Canada, Inc.*, 2022 ONCA 814 and *Winder v. Marriott International, Inc.*, 2022 ONCA 815.

However, under the BC *Privacy Act*, the data defendant could have failed to act when they had an obligation to do so or acted with reckless indifference, causing their liability.

This is a problem. Canadians clearly have different rights and access to defend their rights. Consider the recent PowerSchool hack. In January 2025, PowerSchool, a program used by almost every public-school board in Canada, was hacked, affecting 2.4 million Canadian children.[55] In this instance, some of the most vulnerable Canadians who have very little autonomy over their information were impacted. The Privacy Commissioner of Canada is still investigating.[56] To play out a scenario, if the Privacy Commissioner finds there was a duty that either PowerSchool or specific boards of education failed to ensure their student's privacy rights, then under the current framework, Ontario students could not sue under the common law tort, but BC students could. This example demonstrates the gravity of this issue regarding Canada's access to justice with privacy rights. There should be a federal guideline for all private sector privacy rights. Luckily, the Office of the Privacy Commissioner of Canada set guidelines for all employers.[57] Unfortunately, the Office of the Privacy Commissioner is subjugated to *PIPEDA's* jurisdiction. None of the guidelines are a requirement, and very few private companies follow them.

C. Limited applications of PIPEDA and the Office of the Privacy Commissioner

At this point, this paper has established that Canadians have different privacy rights based on where they live and that they have different pathways to try and defend what rights they have. What's most frustrating is that a federal guideline from the Office of the Privacy Commissioner already exists—and it could potentially fix many problems this paper highlights. Unfortunately, the Office of the Privacy Commissioner is limited to overseeing

[55] Sean Previl, "PowerSchool data breach now at 2.4M Canadian kids. How to protect yourself", *Global News* (January 23, 2025), (https://globalnews.ca/news/10974129/powerschool-data-breach-more-students-impacted/).
[56] See note 46.
[57] Office of the Privacy Commissioner of Canada "Privacy and the Workplace: A Guide for Employers and Employees" *Privacy Topics* Government of Canada, (https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/02_05_d_17/).

federally regulated employers and employees. In the private sector, many fail to follow these guidelines. Private data collection measures are increasing.

In 2022, a Future Skills Centre study by Abacus Data found that 70% of 1,500 remote employees and 500 supervisors experienced digital monitoring.[58] About one-third reported more intrusive surveillance methods like location tracking, video recording, keystroke monitoring, screen captures, or biometric data use.[59] This number has skyrocketed from earlier surveys indicating that about one-third of remote employees were being monitored.[60]

As concerns about employer monitoring grow, Canadians require a guideline that clearly demonstrates what infringes people's privacy. The new guidelines set by the Office of the Privacy Commissioner have a basic outline, especially around consent, which is generally required,[61] but there are exceptions. Consent is not required when collecting, using, or disclosing an employee's personal information if it is essential for establishing, managing, or ending the employment relationship.[62] The office also clarified that individuals cannot waive their privacy rights.[63] When framed in the context of the McMaster University complaint, the notice that the university could use the proctoring information at its discretion would likely not be allowed. However, this new guidance is still vague regarding employer monitoring.

The guidance states that employee monitoring should be specific, targeted, and appropriate in the circumstances, and such monitoring should be necessary for the business to practice.[64] This language is still too vague to inform Canadians of their rights. Canadian Tire

---

[58] Anja Karadeglija, "With AI, workplace surveillance has 'skyrocketed,' leaving Canadian laws behind", *The Globe and Mail,* (March 9, 2024), (https://www.theglobeandmail.com/business/article-with-ai-workplace-surveillance-has-skyrocketed-leaving-canadian-laws/).
[59] See note 56.
[60] Capterra "Workplace Surveillance: A Guide to Employee Monitoring Software" *Capterra* (https://www.capterra.ca/blog/2733/workplace-surveillance-employee-monitoring-software).
[61] Office of the Privacy Commissioner of Canada "Privacy and the Workplace: A Guide for Employers and Employees" *Privacy Topics* Government of Canada, (https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/02_05_d_17/).
[62] *Ibid.*
[63] *Ibid.*
[64] *Ibid.*

could claim that limiting shoplifting is necessary for their business to validate the use of unconsented facial recognition software. Recently, a restaurant in Calgary started requiring its employees to clock in using a fingerprint scanner.[65] Under the current guidance, employers could claim the necessity to avoid "buddy punching" and time theft.

Even if this guideline was imposed on all private companies, the guideline is too vague to make fundamental measurable differences. Canadians are ultimately in a world where they have different privacy rights based on where they live. If they can grapple with what their rights are, the pathways in which they can defend those rights are limited and different based on their location. Even looking at the current federal standards (that only apply to federally regulated businesses), they do not change the issues this paper discussed regarding employer monitoring, biometric data and lack of consent. In the next section, this paper will make some suggestions to help alleviate this access to justice issue.

Legal Reforms and Policy Recommendations

As this paper has outlined, there are three significant issues in the current Privacy law framework. (1) Canadians do not know what their rights are, (2) Canadians do not know how to defend their rights, and (3) The rights Canadians currently have are limited. In this section, this paper will offer some solutions to alleviate these issues.

A. Setting a federal standard for privacy rights

Setting a federal privacy rights standard would balance Canadians' rights. In the current framework, only British Columbia, Alberta, and Quebec have their own provincial privacy statutes.[66] As this paper outlined in the previous section, people who live in these

[65] Phillip Drost, "Biometrics in the workplace may be the way of the future. But at what cost?", *CBC Radio,* (August 25, 2024), (https://www.cbc.ca/radio/costofliving/biometrics-in-workplace-1.7300573).

[66] See Act Respecting the Protection of Personal Information in the Private Sector (CQLR, c. P-39.1) Government of Québec (https://www.legisquebec.gouv.qc.ca/en/document/cs/p-39.1), *Personal Information Protection Act (PIPA)*, RSA 2000, c. P-6.3 Government of Alberta (https://kings-printer.alberta.ca/1266.cfm?page=2003_366.cfm&leg_type=Regs&isbncln=9780779848027), and Personal Information Protection Act (SBC 2003), c. 63, Government of British Columbia (https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_03063_01).

provinces have more privacy rights. This should not be the case. A simple solution would be to create a federal standard for privacy rights across Canada. Bill C-27 is Canada's attempt to solve this problem.

Bill C-27 is a significant step forward, assuming it will eventually be passed. But it demonstrates how late Canada is in rectifying this. Suppose Canada creates and enforces the digital charter in 2026. In that case, it will be eight years after the European Union implemented the *GDPR* and twenty-two years after Alberta and BC implemented their *PIPA* legislations. Further, if Bill C-27 is implemented as it is currently written, it still has a limited pathway for individuals to defend their rights. It also has limited rights that mirror the current *PIPEDA* guidelines.[67]

B. Creating a standardized tort to defend privacy rights

Bill C-27 currently states that if someone feels their privacy rights have been infringed, they have the right to issue a complaint to either their organization or the Office of the Privacy Commissioner. There is no framework establishing a right to sue under a federally recognized tort. The Office of the Privacy Commissioner is already overwhelmed with privacy complaints and takes years to investigate and decide. Under *PIPEDA*, the office has one year to issue a report on the findings.[68] Yet many recent investigations have not been completed in that time limit. They began investigating TikTok in February 2023 with no results to show so far.[69] The same goes for Open AI in May of 2023.[70] They are still

[67] Library of Parliament "Bill C-27: The Digital Charter Implementation Act, 2022 – Legislative Summary" *Parliament of Canada,* at ss. 2.1-2.4. (https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/441C27E).
[68] Office of the Privacy Commissioner, "Guide to PIPEDA complaint processes", (https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/guide/#).
[69] Office of the Privacy Commissioner, Announcement (https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230223/).
[70] Office of the Privacy Commissioner, Announcement (https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230525-2/).

investigating ArriveCAN as well.[71] Under the current framework, their oversight is only over federally regulated businesses. If their scope is also expanded to all private businesses, many complaints will likely never be heard or investigated.

This paper earlier demonstrated the difference between the tort of intrusion upon seclusion and the BC *Privacy Act*. Both pathways have benefits and drawbacks. Bill C-27 should have a written policy that outlines a federally approved pathway for individuals to defend their rights. An act like the BC *Privacy Act* could be added to the bill. This would decrease the burden on the privacy commissioner while also giving a standardized pathway all Canadians could follow. The Act should hold data defendants accountable for negligent breaches of information. It should make companies vicariously liable to ensure that private sectors take these rights seriously. And it should include intrusions to be willful or reckless to adopt the better language from the ONCA. Adding this would help Canadians defend their rights, but Canadians should have more rights than the current framework shows.

C. Strengthening privacy rights

This paper will make a final suggestion to strengthen people's privacy rights. Bill C-27 mirrors the current *PIPEDA* framework and applies it to private entities.[72] As this paper outlines, the *PIPEDA* framework is vague, especially regarding employer surveyance. A framework that explains what is necessary for business operations to collect personal information is needed. Currently, some privacy commissioners hold high privacy rights, such as the Canadian Tire example. But others, like McMaster University, have not been held in the same regard.

Under the *GDPR*, individuals not only have the right to file complaints and defend their privacy rights, but they also have the right to request the deletion of personal

[71] Office of the Privacy Commissioner, Announcement (https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/an_240319/#).
[72] See note 57.

information or to see what information an organization has about them. Under the current bill C-27 framework, Canada would not have those rights, and *PIPA* regulation in BC and Alberta does not, either.[73] To ensure the efficiency of these processes, Canada needs to arm its citizens with tools so they can defend their privacy rights independently.

Conclusion

Canada still has significant progress to make in ensuring that all Canadians have equal access to justice in protecting their privacy rights. The fact that these rights vary depending on where one lives is both inconsistent and unjust. As a society, we are increasingly recognizing that privacy is not just a policy issue—it is a fundamental right central to our democratic values. To fully recognize this, Canada must adopt comprehensive federal legislation that not only standardizes access to justice across provinces but also upholds our dignity and protects our fundamental freedoms.

[73] Fasken "Comparative Table of Personal Information Protection Laws" *Fasken* (https://www.fasken.com/en/knowledge/2022/07/26-comparative-table-of-personal-information-protection-laws#authors).

References

Legislation

Act Respecting the Protection of Personal Information in the Private Sector, CQLR, c. P-39.1 (Government of Québec)."

Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, 1st Sess, 45th Parl, 2025 (first reading 18 June 2025).

Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 44th Parl, 2022 (first reading 14 June 2022)."

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, 44th Parl, 2022 (first reading 16 June 2022).

Bill C-63, *An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide Internet service and to make consequential and related amendments to other Acts*, 1st Sess, 44th Parl, 2024 (first reading 26 February 2024).

Employment Standards Act, RSBC 1996, c 113.

Personal Information Protection Act, SBC 2003, c 63.

Personal Information Protection Act (PIPA), RSA 2000, c P-6.3 (Government of Alberta).

Privacy Act, R.S.C, 1985, c P-21.

Privacy Act, RSBC 1996, c. 373.

Regulation (EU) 2016/679 General Data Protection Regulation, OJ L 119, 1.

Jurisprudence

Campbell v Capital One Financial Corporation, 2024 BCCA 253.",

Canadian Tire Associate Dealers' use of facial recognition technology Re, Investigation Report 23-02, 2023 BCIPCD No 17.

G.D. v South Coast British Columbia Transportation Authority, 2024 BCCA 252.

Insurance Corporation of British Columbia v. Ari, 2023 BCCA 331.

Jones v. Tsige, 2012 ONCA 32.

McMaster University Re, Privacy Complaint PI21-00001, 2024 OIPC No 39.

Obodo v. Trans Union of Canada, Inc., 2022 ONCA 814.

Odhavji Estate v Woodhouse, 2003 SCC 69.

Owsianik v. Equifax Canada Co., 2022 ONCA 81.

Peracomo Inc. v TELUS Communications Co., 2014 SCC 29.

R. v Cole, 2012 SCC 53.

Situmorang v Google, LLC, 2024 BCCA 9.

Winder v. Marriott International, Inc., 2022 ONCA 815.

Zablotney v. British Columbia, 2023 BCCA 31.

Secondary Materials

Blakes, "Digital Policy Issues Face Uncertain Future After Prorogation of Parliament\" (26 January 2025), online: Blakes <https://www.blakes.com/insights/digital-policy-issues-face-uncertain-future-after-prorogation-of-parliament>.

Canada Revenue Agency, "Info Source – Appendix\" (2025), online: Government of Canada <https://www.canada.ca/en/revenue-agency/corporate/about-canada-revenue-agency-cra/access-information-privacy-canada-revenue-agency/info-source-appendix.html>.",

Canada, Library of Parliament, Legislative Summary of 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, Publication No 44-1-C27-E (2022), online: <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/441C27E>.

Capterra, "Workplace Surveillance: A Guide to Employee Monitoring Software", online: Capterra <https://www.capterra.ca/blog/2733/workplace-surveillance-employee-monitoring-software>.

Data Guidance, "Canada: Bill C-27 dies after Parliament is prorogued" (12 February 2025), online: Data Guidance.

Department of Justice Canada, "Modernization of the Privacy Act", Justice Laws Website, online: Government of Canada https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html#s1.

Department of Justice Canada, "Personal Information Protection and Electronic Documents Act (PIPEDA)", online: Government of Canada <https://laws-lois.justice.gc.ca/PDF/P-21.pdf>.",

Drost, Phillip, "Biometrics in the workplace may be the way of the future. But at what cost?" CBC Radio (25 August 2024), online: <https://www.cbc.ca/radio/costofliving/biometrics-in-workplace-1.7300573>.

Fasken, "Comparative Table of Personal Information Protection Laws", online: Fasken <https://www.fasken.com/en/knowledge/2022/07/26-comparative-table-of-personal-information-protection-laws/authors>.

Gowling WLG, "Critical infrastructure cyber security bill" (19 June 2025), online: Gowling WLG <https://gowlingwlg.com/en-ca/insights-resources/articles/2025/critical-infrastructure-cyber-security-bill>.

Gowling WLG, "Federal privacy reform: Where we left off and what's next" (25 September 2025), online: Gowling WLG <https://gowlingwlg.com/en-ca/insights-resources/articles/2025/federal-privacy-reform>.

Gowling WLG, "Privacy and cyber bills: What to expect post-election" (24 April 2025), online: Gowling WLG <https://gowlingwlg.com/en-ca/insights-resources/articles/2025/privacy-and-cyber-bills-what-to-expect-post-election>.

Karadeglija, Anja, "With AI, workplace surveillance has skyrocketed, leaving Canadian laws behind", The Globe and Mail (9 March 2024), online: <https://www.theglobeandmail.com/business/article-with-ai-workplace-surveillance-has-skyrocketed-leaving-canadian-laws>.

McMillan LLP, "OPC Takes Firm Stance on Privacy in the Workplace: Takeaways for Employers", online: McMillan <https://mcmillan.ca/insights/publications/opc-takes-firm-stance-on-privacy-in-the-workplace-takeaways-for-employers>.

Office of the Privacy Commissioner of Canada, Announcement (23 February 2023), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230223>.

Office of the Privacy Commissioner of Canada, Announcement (25 May 2023), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230525-2>.

Office of the Privacy Commissioner of Canada, Announcement (19 March 2024), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/an_240319>.

Office of the Privacy Commissioner of Canada, \"Guide to PIPEDA complaint processes\", online: <https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/guide>.

Office of the Privacy Commissioner of Canada, "Personal Information Protection and Electronic Documents Act (PIPEDA) – Overview: Privacy Laws in Canada", online:

Government of Canada <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r-o-p>.

Office of the Privacy Commissioner of Canada, "PIPEDA: A Brief Overview: Privacy Laws in Canada", online: Government of Canada <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief>.

Office of the Privacy Commissioner of Canada, "Privacy and the Workplace: A Guide for Employers and Employees: Privacy Topics", online: Government of Canada <https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/02_05_d_17>.

Parsons Corrin LLP, "ICBC Privacy Breach Class Action", online: Parsons Corrin <https://parsonscorrin.ca/practice-areas/class-actions/icbc-privacy-breach-class-action>.

Previl, Sean, \"PowerSchool data breach now at 2.4M Canadian kids. How to protect yourself\", Global News (23 January 2025), online: <https://globalnews.ca/news/10974129/powerschool-data-breach-more-students-impacted>.

Shull, Aaron, "Safeguarding Privacy and Preserving Freedom of Thought in Canada: A Call to Action", Centre for International Governance Innovation (28 March 2024), online: <https://www.cigionline.org/articles/safeguarding-privacy-and-preserving-freedom-of-thought-in-canada-a-call-to-action>.

Tech Policy Press, "Canada's Online Harms Bill is Dead Again" (29 April 2025), online: Tech Policy Press <https://techpolicy.press/canadas-online-harms-bill-is-dead-again-three-questions-to-consider-for-the-next-round>.