# Canadian Privacy Law Review

VOLUME 22, NUMBER 5 Cited as (2025), 22 C.P.L.R. APRIL 2025


## • LOOKING AHEAD: THE CANADIAN PRIVACY AND AI LANDSCAPE WITHOUT BILL C-27 •


Nic Wall, Senior Associate, Molly Reynolds, Partner, Rosalie Jetté, Associate, Julie Himo, Partner, Lauren Nickerson, Associate, and Mavra Choudhry, Associate, Torys LLP .



**Nic Wall**

**Molly Reynolds**

**Rosalie Jetté**

**Julie Himo**

**Lauren Nickerson**

**Mavra Choudhry**

**With** the prorogation of Parliament last week, Bill C-27, including the new AI law and proposed privacy reforms it contained, "died". No new federal privacy or AI legislation is likely to pass anytime soon. However, privacy and AI standards—and therefore risks of non-compliance—continue to evolve. This article surveys the privacy and AI landscape with Bill C-27 no longer on the horizon.

WHAT YOU NEED TO KNOW

- While no new federal privacy or AI legislation is likely to pass this year, Canadian organizations should continue to monitor the constantly evolving privacy and AI landscape.

### • In This Issue •




LexisNexis®

**CANADIAN PRIVACY LAW REVIEW**

**Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.



**ISBN 0-433-44417-7 (print) ISSN 1708-5446**
**ISBN 0-433-44650-1 (PDF) ISSN 1708-5454**
**ISBN 0-433-44418-5 (print & PDF)**

Please address all editorial inquiries to:

**General Editor**
Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

**LexisNexis Canada Inc.**
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: cplr@lexisnexis.ca
Web site: www.lexisnexis.ca



- Recent provincial reforms in Québec and elsewhere are likely to continue impacting organizations as this evolution informs industry standards, even for businesses with limited operations in those provinces.
- Regulatory action and guidance indicate certain priority areas—including AI, biometrics, deceptive design practices, and protection of children's and health information—that are likely to receive increased investigative scrutiny.
- Trends in class action litigation indicate increasing risk associated with intentional data use and AI initiatives.
- International laws and standards also influence practices, expectations and risks in the Canadian market.

## PROVINCIAL LAWS

### Québec

Québec's *Act respecting the protection of personal information in the private sector* (**"Law 25"**), the final component of which came into force in September 2024, will continue to be a major influence on privacy requirements for several reasons. First, Law 25 contains the most significant penalty provisions of any privacy law in Canada—up to $10 million or 4% of an organization's global revenue. It also has a broad potential scope of extraterritorial application and contains some of the most stringent and prescriptive requirements.

In light of these factors, many organizations have elected to apply Québec's standards and rights to all data subjects, even when those data subjects are located outside of Québec. Some of these organizations prefer a single, harmonized set of requirements; others lack an effective means of identifying a data subject's province and delineating their processes accordingly. In some cases, organizations that were not subject to Law 25 also chose to adopt Québec-compliant practices, with the objective of gaining a competitive advantage and fostering important business relationships with partners who are subject to Law 25. We therefore expect to see Law 25 continue to influence industry practice,

even when the law does not directly apply in the circumstances.

### Ontario

The June 2021 release of the Ontario government's white paper on privacy reform[1] was accompanied by comments from the then-Minister of Government and Consumer Services indicating that if federal privacy reform was insufficient, the Ontario government would possibly step in. There have been no public statements indicating this intention recently.

However, the Ontario government has shown recent willingness to legislate on both privacy and AI. In November, the government passed the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*. This Act creates new regulation-making powers regarding public sector cybersecurity and use of AI. Another component of this reform would, once proclaimed, expand the Ontario Information and Privacy Commissioner's investigative powers with respect to public institutions. Ontario has also passed legislation that, once in force, would require employers to disclose the use of AI in their hiring process.

### Alberta

Alberta recently passed reforms to its public sector privacy law, the *Freedom of Information and Protection of Privacy Act*, with the enactment of Bill 33. Bill 33, the *Protection of Privacy Act*, includes strengthened privacy protections and new rules with respect to data use and sharing. It also includes increased penalties (up to $750,000 for an organization), which the Alberta government is hoping will give some teeth to a statute that had not been looked at in over two decades.

While Alberta's private sector privacy law, the *Personal Information Protection Act* (**"PIPA"**) is still currently under review, the approach taken by the government for the public sector legislation, as well as the support it has received from the provincial privacy commissioner, may indicate an appetite for private sector reform, too.

## REGULATORY ACTION AND GUIDANCE

Regulatory action and guidance continue to influence standards in privacy and AI. For example, in December 2023, the Office of the Privacy Commissioner of Canada (**"OPC"**), jointly with all Canadian provincial and territorial privacy regulators, released guidance on generative AI entitled Principles for responsible, trustworthy and privacy-protective generative AI technologies.

Other recent actions by OPC and other privacy regulators can be taken as indicative of enforcement priorities. In addition to the use of generative AI, these include:

- children's privacy;
- biometrics;
- deceptive design practices;
- collection and use of data for AI training;
- protection of personal health information; and
- employee surveillance.

Privacy concerns regarding these topics will be subject to higher degrees of regulatory scrutiny. This heightened regulatory risk in turn creates heightened litigation and reputational risk.

Many other regulators have also taken actions that indicate AI will be subjected to heightened scrutiny. For example, the Competition Bureau has signaled its intention to continue monitoring the use of AI and its impact on competition and identified concerns about certain potential uses of AI including algorithmic pricing, algorithmic collusion, and the use of deepfakes. Human rights watchdogs, such as the Ontario Human Rights Commission, have flagged the potential for bias and discrimination in AI systems. Furthermore, the Office of the Superintendent of Financial Institutions and the Financial Consumer Agency of Canada recently released a joint report on the risks of AI in federally regulated financial institutions.[2]

Generally, Canadian regulators have emphasized the importance of cross-sector collaboration given the complex and multifaceted nature of AI regulation, particularly in the areas of privacy, competition, telecommunications, and intellectual property.

## CLASS ACTION LITIGATION

### Privacy Class Actions

Broadly speaking, the last few years have seen an increasingly sophisticated class action plaintiffs' bar expand beyond class action claims based on data breaches to include an organization's intentional data handling practices. For example, claims may be based on an allegation of the collection, use, or disclosure of personal information without sufficient consent. Such data handling claims can be based in tort, contract or statute. Ultimately, this means that the litigation risk for data handling practices involving a large number of individuals is higher than it was several years ago and continues to increase.

### AI Class Actions

The intersection of AI and class action litigation is also growing. Such class actions include:

- privacy-related claims, such as the use of AI to improperly obtain biometric identifiers of individuals;
- employment and discrimination-related claims, such as discrimination in the hiring process stemming from the use of AI;
- anti-trust and competition-related claims, such as the use of AI leading to price-fixing or market manipulation;
- insurance-related claims, such as the improper use of AI to make insurance claim determinations; and
- intellectual property-related claims, such as the unlicensed use of copyrighted material to train AI systems.

## INTERNATIONAL AI LAWS AND STANDARDS

International laws can be influential in setting standards and expectations, particularly for organizations operating in multiple jurisdictions that seek a harmonized privacy or AI governance program. Note, however, that in the absence of major changes to the international privacy landscape, this section focuses on AI laws and standards.

### European Law

The European Union's *Artificial Intelligence Act* (**"AIA"**) is a prime example. The AIA came into force in August 2024 and is set to take effect incrementally over the next two years. The AIA imposes obligations pertaining to risk management, data governance, documentation and record-keeping, human oversight, cybersecurity, transparency, and quality control, among others. Its scope of application includes providers and deployers of AI systems located outside the EEA whose AI outputs are used within the EU. This means that, like the EU's data privacy regulations (known as the GDPR), the AIA can apply to Canadian businesses with operations or customers in the EEA. Over the last several years, the GDPR has had a significant impact on global privacy practices and the AIA is expected to be similarly influential on AI standards.

### United States Law

There is currently no proposed comprehensive federal AI-specific legislation in the U.S. In 2023, the Biden White House issued an executive order concerning the safe and secure use of AI that addressed privacy, security, equity, and human rights concerns, but the incoming Trump administration has signaled its intention to both repeal this order and oppose regulation that could interfere with AI innovation. However, as in privacy law, a patchwork of state AI laws is emerging. Three states have been leading the pack for legislation governing the private sector: Utah, Colorado and California. These three states adopted legislation in 2024 which include requirements with respect to governance and transparency related to the use of AI.

In addition, Illinois, Massachusetts and Ohio have several active bills that are currently being reviewed at the committee level.

### Other Jurisdictions

The United Kingdom's government recently announced its intention to introduce AI legislation, which is anticipated sometime this year.

The South Korean National Assembly recently passed the *Basic Act on the Development of Artificial Intelligence and the Establishment of Trust*, which will take effect in January 2026. Taiwan, Brazil, and Chile have also introduced draft AI legislation. Like the AIA, each of these instruments will impose different regulatory obligations based on an AI system's presumed level of risk.

### International Standards

In 2023, the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce, published a voluntary set of guidelines titled the *AI Risk Management Framework*, with the goal of managing AI-related risk and increasing trustworthiness in the design, development, and use of AI systems.

The International Standards Organization has also released certain standards, including ISO/IEC 42001, 23894, and 38507. ISO/IEC 42001, released in December 2023, specifies requirements for establishing, implementing, maintaining, and continually improving an AI management system to help ensure responsible development and use.

While these international standards are non-binding, they can nevertheless inform expectations. Businesses may inquire about compliance with such standards as part of a due diligence exercise, or contractually require compliance when acting as a customer for an AI-based product or service. Moreover, these standards have the potential to indirectly inform legal obligations, such as a company's standard of care in a negligence claim.

## IMPLICATIONS FOR BUSINESSES

The privacy and AI landscape continues to rapidly evolve, even in the absence of Bill C-27. Canadian organizations should continue to monitor this landscape, particularly given the pace of change.

For the sake of efficiency, many organizations were delaying some of their privacy and AI compliance initiatives until the requirements of Bill C-27 crystallized. However, with Bill C-27 no longer on the horizon, organizations should revisit their compliance initiatives to identify and address key risk areas and establish a list of priorities for 2025. For privacy compliance, special attention should be paid to Law 25 requirements and recent regulatory actions and decisions. AI governance programs should align with best practices to help limit risk, meet existing industry expectations and reduce the compliance burden as new AI laws are passed.

[***Nic Wall*** *is a Senior Associate at Torys LLP in Toronto, ON. Nic's practice focuses on privacy, cybersecurity and data governance. He regularly advises clients on privacy law and AI compliance and matters of data rights and protection, as well as represents clients in regulatory complaints and investigations, administrative proceedings and civil litigation.*

***Molly Reynolds*** *is a Partner at Torys LLP in Toronto, ON. Molly has a deep and nuanced understanding of privacy law compliance, as well as data security best practices, breach response, regulatory investigations, and privacy class action defence. She represents clients in administrative proceedings under access to information, anti-spam and privacy legislation, as well as in the context of civil litigation.*

***Rosalie Jetté*** *is an Associate at Torys' Montréal office. Rosalie's practice focuses on providing practical and strategic support to clients on privacy, cybersecurity, data governance and consumer law. She regularly advises clients on privacy law compliance and data governance in the context of their day-to-day operations, new initiatives and commercial transactions, as well as on data breach preparedness and response.*

***Julie Himo*** *is a Partner at Torys' Montréal office. Julie frequently acts as breach coach for clients and has considerable experience with all types of cyber incidents, including coordinating notification and regulatory filing efforts across multiple countries. In addition to her breach coach work, Julie conducts strategic risk and privacy assessments, and has extensive experience in commercial litigation.*

***Lauren Nickerson*** *is an Associate at Torys LLP in Toronto, ON. Lauren's work focuses on the*

*evolving intersection between artificial intelligence and the law. She collaborates with practice groups across the firm to provide insight on emerging legal issues, including matters related to AI governance, regulatory compliance and risk mitigation.*

***Mavra Choudhry** is an Associate at Torys LLP in Toronto, ON. Mavra's practice focuses on privacy and data protection related matters. Mavra regularly advises clients on privacy compliance, data breach response protocol and litigation arising from breaches.*]

[1] Government of Ontario, online: https://www.ontariocanada.com/registry/showAttachment.do?postingId=37468&attachmentId=49462

[2] Office of the Superintendent of Financial Institutions, online: https://www.osfi-bsif.gc.ca/en/about-osfi/reports-publications/osfi-fcac-risk-report-ai-uses-risks-federally-regulated-financial-institutions

## • USE OF BIOMETRIC DATA: QUÉBEC'S PRIVACY COMMISSIONER KEEPS THE BAR HIGH •

Caroline Deschênes, Partner, Ilona Bois-Drivet, Lawyer, Antoine Rancourt, Partner,
Marc-Alexandre Hudon, Partner, Langlois LLP



**Caroline Deschênes**


**Ilona Bois-Drivet**


**Antoine Rancourt**


**Marc-Alexandre Hudon**

**The** use of biometrics is growing in both the private and public sectors. In its latest progress report (2023-2024), Quebec's privacy commissioner, the *Commission d'accès à l'information* (**"CAI"**), stated that it received 124 declarations (including 118 from businesses), which represents an increase of 59% over the previous year. While this increase can be partly attributed to the fact that the *Act to modernize legislative provisions as regards the protection of personal information* (**"Law 25"**) includes a requirement to notify the CAI before using biometric data (an obligation that was previously limited to the creation of a biometric database), we can certainly expect this trend to continue over the next few years.

For the first time since Law 25 came into force, the CAI has had the opportunity to render a decision on the use of a facial recognition system by a business in the printing sector. The decision, published late last year, is only the tenth in this

area. It is another illustration of the CAI's rigorous standards regarding biometric systems.

## QUÉBEC'S LEGAL FRAMEWORK FOR BIOMETRICS

The use of biometric information (images, fingerprints, voice, hand shape, etc.) is governed by a double legislative framework. On the one hand, the *Act respecting the protection of personal information in the private sector* (the **"Private Sector Act"**) (for businesses) or the *Act respecting access to documents held by public bodies and the protection of personal information* (the **"The Access Act"**) (for public bodies) applies whenever an organization uses biometric information to identify a person directly or indirectly. On the other hand, the *Act to establish a legal framework for information technology* (the **"Quebec IT Act"**) stipulates that any organization wishing to use a biometric system to verify or confirm an individual's identity or to create a database of biometric characteristics or measurements is also subject to the requirements of the Quebec IT Act.

The Private Sector Act and the Access Act do not specifically address biometrics, except to stipulate that biometric information constitutes sensitive information. However, the other obligations applicable to personal information, such as collecting only the necessary information and being transparent, do apply to the processing of biometric data.

The Quebec IT Act imposes specific obligations concerning biometrics, including:

(a) the express consent of the persons concerned and;

(b) prior disclosure to the CAI. A declaration form (in French only) is available on the CAI website for this purpose.

The Quebec IT Act also stipulates that the biometric system must only use the minimum number of characteristics or measurements required for identification.

Under these laws, the CAI has investigation and inspection powers. With regard to biometric databases, the Quebec IT Act provides that the CAI may issue orders determining how such data is to be set up, used, consulted, released and retained, as well as how it is to be archived or destroyed. Should a database be found to be non-compliant with the law, the CAI may also suspend or prohibit the bringing into service of such a database or order that it be destroyed.

## THE CAI'S RECENT DECISION

In October 2020, a company Transcontinental Printing Inc. (the **"Company"**) informed the CAI that it had created a biometric database as part of its implementation of a facial recognition system aimed at controlling access to its premises to ensure their security and, incidentally, meet the requirements of the Customs-Trade Partnership Against Terrorism (the **"CTPAT"**) certification. The CAI investigated the Company's practices and ordered that it cease collecting and using biometric information.

To assess the legality of creating a biometric database and using a facial recognition system, the CAI used a two-stage necessity test (the **"Necessity Test"**). The Company must demonstrate that:

1. The objective pursued by the data collection is **legitimate, important and real;**
2. The invasion of privacy is **proportionate** to the intended objective.

Although the Company obtained the consent of its employees to use their biometric information, the CAI reiterated that a company isn't exempt from these requirements, even with the consent of the person concerned.

### 1. Is The Objective Legitimate, Important and Real?

The CAI considers it legitimate for the Company to want to ensure its facilities' security and take measures to control access to its premises.

As to whether the database serves a real objective, the CAI considered that the information provided by the Company failed to establish any specific incident, problem or security issue. Firstly, the CAI considered that the Company's compliance with the CTPAT standard does not require using facial recognition; even if this method was suggested,

the standard allows for less intrusive means of controlling access to premises. Moreover, the CAI noted that the risk of copying and sharing identification cards, which the Company cited as an alternative means of controlling access to its premises, is hypothetical and does not constitute a real problem experienced by the Company.

As to the importance of the objective, the CAI considers controlling access to a business' premises a standard business objective. While the CAI recognized that a business' operations or a particular situation might justify a higher level of security, such as that provided by biometric systems, it considered that the Company's operations in the printing industry do not appear to present any particular risks that would require such a level of security.

### 2. Is The Invasion of Privacy Proportional to the Stated Objective?

To assess the proportionality test, the CAI places the burden on the Company to establish that:

1. The data collection is rationally connected to the stated objective;
2. The level of invasion of privacy caused by the collection of personal information is minimized;
3. Collecting this personal information is clearly more useful to the Company than harmful to the persons concerned.

The CAI considers that collecting biometric information for use in a facial recognition system is rationally connected to controlling access to the Company's premises.

However, the Company must ensure that it minimizes the invasion of privacy by assessing the possibility of using other, less intrusive means. The CAI reiterated that the risk alleged by the Company regarding the copying or lending of identification cards is hypothetical. It considered that the Company had provided no evidence that an access card could be copied, and expressed the opinion that the inconvenience associated with managing the loss and replacement of cards was part of standard business practice. It found that other, less privacy-intrusive means were available to the Company to control access to the premises.

Finally, the CAI found that the Company failed to demonstrate how the benefits of collecting personal information to operate the biometric system outweighed the invasion of privacy associated with the collection.

### COMMENT

This decision again demonstrates the CAI's stringent requirements regarding the use of biometric systems and its strict interpretation of the necessity criterion in this context. The CAI also reaffirms the importance of documenting the necessity of collecting biometric information, even if an organization has the consent of the persons concerned and implements security measures.

It is worth noting that, with one exception, CAI decisions have consistently found that the use of biometrics does not meet the Necessity Test criteria. In addition to the decision discussed in this article, the CAI has not deemed the collection of biometric information to be necessary for the following purposes:

- Improved payroll management (*Auberge Sacacomie*)
- Employee identity verification and improved management of working hours (*Selenis Canada*)
- Reducing the business' environmental footprint, improving the customer experience and reducing fraud (*Les 3 Piliers Inc.*)
- Commercial use (*Clearview AI*)
- Preventing a business-wide COVID-19 outbreak and quickly identifying employees with a fever (*Héritages Ébénisterie)*

In the only decision in which the CAI ruled that the necessity criterion was met (*Marché d'alimentation Marcanio et fils inc*), it concluded that the use of biometrics to monitor employee hours satisfied both stages of the Necessity Test because very specific facts had been demonstrated:

- The manager could not be present to cover all the time slots of the employees under his supervision, given the number of employees, their varying schedules from week to week, and their different work areas;

- Prior to implementing the system, the business fell victim to time theft (fraud) and had dismissed employees for this reason;
- Employees who didn't have their card with them had to ask a supervisor to register their time in the time clock, leading to lost time for the employees and the business;
- Alternative measures to biometrics had been considered, but those were too costly and difficult to implement in their specific work environment;
- The introduction of the biometric system years earlier had eliminated time theft and lost time.

The CAI's recent decision aligns with the principles set out in its previous decisions as well as the CAI's guide to biometrics for organizations (the **"Guide"**) (available in French only). While the Guide isn't legally binding, it does highlight the CAI's position on the issue. Among other things, the CAI insists that the use of biometrics must **address a problematic situation** and that the organization must **specify and document the problem encountered** in the pursuit of its objective. It is clear from the CAI decisions that the demonstration of the problem or situation to be solved must be based on tangible and convincing facts.

Does this mean that the organization must demonstrate that it has already suffered the disadvantages or risks that biometrics seeks to resolve? The CAI seems to suggest this in the present decision, pointing to a lack of evidence of identification cards being copied or lent and concluding that this is a "hypothetical risk."

In our opinion, to meet the Necessity Test criteria, it should not be necessary to demonstrate that the incident has already occurred but rather that biometrics seek to resolve an **important and real issue**, even if that issue has yet to occur. For instance, consider a facility where radioactive metals are stored. In order to demonstrate the need for access control using reliable biometric technology, it would be unreasonable to demand proof that a security breach has already occurred. Similarly, in an industry where it is standard practice to use a biometric system to authenticate or identify employees or customers, the question is whether the harm sought to be prevented by the use of a biometric system should be required to have occurred in order to satisfy the Necessity Test. Indeed, it should be noted that organizations have an obligation to put reasonable security measures in place to protect the personal information they hold, and industry standards may be relevant in determining what measures are reasonable.

Lastly, while regulators agree on the challenges posed by biometrics, their approach seems to include some nuances. On the necessity criterion, the Office of the Privacy Commissioner of Canada (the **"OPC"**) appears to take a slightly more flexible approach than the CAI. The necessity criterion is echoed in the *Draft Guidance for processing biometrics—for organizations*, which was recently the subject of a consultation process. The OPC states that the organization must demonstrate that "the biometric program or initiative is necessary to meet a specific, legitimate and defensible need." The OPC advises organizations to consider whether their "needs are rationally connected to a business goal that is pressing or substantial" and to document this clearly. The OPC believes the initiative should not go forward if the organization cannot explain how the "collection, use, or disclosure of biometrics is rationally connected to a pressing and substantial business goal."

In conclusion, before making the mandatory declaration to the CAI, it is recommended that organizations planning to use biometrics:

- Pay particular attention to **justifying** the intended objective by **documenting the real problems or issues** to be resolved, the connection between collecting biometric information and the objective, and the proportionality of the collection to this objective. It is also useful to document the **alternative means considered** and the reasons why these are not appropriate in the circumstances, with reference to specific—not hypothetical—facts. In this respect, it is useful to consider the CAI's positions as expressed in the Guide and the decisions cited above.
- Carry out a Privacy Impact Assessment (a **"PIA"**) to demonstrate the risk analysis and mitigation measures in place and the

organization's compliance with the legal obligations associated with particularly sensitive biometric information. Indeed, since September 2023, a PIA is mandatory for all projects involving the acquisition, development, or overhaul of information systems or the electronic service delivery systems involving the collection, use, communication, retention, or destruction of personal information.

- Finally, organizations would be well advised to seek **legal support** for these steps, given the sensitivity of biometric information and the CAI's rigorous and restrictive approach.

[***Caroline Deschênes**, CIPP/C, CIPM, specializes in privacy, cybersecurity, and access to information. She advises clients of all sizes across various industries on establishing and implementing privacy compliance programs, managing confidentiality incidents, interacting with regulatory bodies, and complying with Canada's anti-spam legislation. Caroline is an active member of the executive committee of the Privacy and Access Law Section of the Canadian Bar Association, which she chaired in 2022-2023. Her expertise in data protection and privacy has been recognized by several respected legal directories.*

***Ilona Bois-Drivet** dedicates her practice exclusively to technology, privacy and data governance law, and legal matters relating to artificial intelligence. She helps businesses and organizations of all sizes comply with Québec and Canadian privacy laws and advise clients on all areas of personal information protection that relate to artificial intelligence (AI).*

***Antoine Rancourt** is a business lawyer with an expertise in technology, intellectual property, privacy law, and data governance. Tech companies call on him for advice on commercializing, protecting, and leveraging their technologies. Antoine helps businesses and organizations of all sizes comply with Canadian and Québec privacy and anti-spam laws and provides guidance on how to manage databases and process and store personal information through its life cycle. He is also involved in various corporate transactions on a regular basis, especially in the technology sector.*

***Marc-Alexandre Hudon** is a member of both the Litigation and the Corporate and Commercial Law groups. His practice focuses primarily on the protection of personal information, cybersecurity, AI, public contracts, business integrity and administrative law. He acts for a wide range of clients, particularly in the natural resources and energy, infrastructure, health, and technology sectors. A seasoned litigator before both Québec courts and the Federal Court, he assists clients with investigations, transactions, and various related matters*.]

## • BEYOND BORDERS: BC COURT ISSUES SEMINAL RULING ON THE JURISDICTIONAL APPLICATION OF THE *PERSONAL INFORMATION PROTECTION ACT* •

Lyndsay A. Wasser, Partner, Kristen Pennington, Partner, Robbie Grant, Associate, McMillan LLP




**Lyndsay A. Wasser** **Kristen Pennington** **Robbie Grant**

**In** a much-anticipated decision that may have ripple effects in other jurisdictions, the British Columbia Supreme Court has provided clear guidance on the application of the *Personal*

*Information Protection Act*, S.B.C. 2003, c. 63 (**"BC PIPA"**) to foreign organizations.

In *Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia*, the Court upheld the Office of the Information and Privacy Commissioner for British Columbia's (**"OIPC"**) order against Clearview AI Inc. (**"Clearview"**), a U.S.-based facial recognition company, in connection with Clearview's violations of BC PIPA.[1]

The Court's ruling establishes that BC PIPA applies to organizations outside of British Columbia (**"BC"**) that have a "real and substantial connection" to BC. Although this finding appears to support a contextual analysis similar to the test applied when considering the application of the federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (**"PIPEDA"**) to organizations outside Canada, the BC Court expressed the view that a sufficient connection can be established for the purposes of BC PIPA merely by collecting data from individuals in BC through the Internet.[2]

## BACKGROUND

Clearview operates a facial recognition system that scrapes publicly accessible images from social media and other online platforms, which it then converts into biometric identifiers. Clearview's business involves selling software to law enforcement agencies and private sector entities, which allows them to match faces to the images in Clearview's searchable biometric database. At the time that Clearview's activities came to the attention of Canadian privacy regulators, the company had amassed over three billion facial images, including those of persons in BC, without their consent. Clearview's own website currently claims that its database contains over 50 billion facial images collected from the Internet (an average of six per person on the planet).[3]

In 2020, the Office of the Privacy Commissioner of Canada (**"OPC"**), along with the OIPC and the privacy commissioners in Alberta and Quebec, investigated Clearview for violations of Canada's privacy laws, culminating in a joint investigation report (the **"Joint Investigation Report"**). The Joint Investigation Report found that Clearview contravened Canadian private-sector privacy legislation and included specific compliance recommendations for Clearview.[4]

That same year, Clearview voluntarily suspended its services to Canadian users. However, the company suggested that the suspension was intended to be temporary, and Clearview continued to collect and store images of Canadians.[5]

### The OIPC's Order

In 2021, the OIPC issued an order requiring Clearview to comply with the recommendations of the Joint Investigation Report. The Alberta and Quebec privacy regulators made similar orders within their own jurisdictions. Specifically, the OIPC's order required Clearview to:[6]

1. Stop offering its facial recognition services in BC;
2. Make best efforts to cease collecting, using, or disclosing images and facial recognition data of individuals in BC without their consent; and
3. Make best efforts to delete previously collected images and facial recognition data that was collected from individuals in BC without their consent.

Clearview challenged the OIPC's order, arguing that it is not subject to BC PIPA because it does not engage in business activities within BC. In particular, Clearview focused on the fact that it has no employees, offices, or servers in BC.

In the alternative, Clearview argued that the order should be quashed because: (i) the personal information collected from online sources was "available to the public" pursuant to BC PIPA and related regulations, and therefore, Clearview did not need consent to collect the information; (ii) contrary to the findings in the Joint Investigation Report, a reasonable person would consider Clearview's purpose for collecting, using and disclosing personal information to be appropriate in the circumstances; and (iii) the OIPC's order was unnecessary and unenforceable.[7]

## THE COURT'S FINDINGS

### The Extraterritorial Jurisdiction Test

In the Joint Investigation Report, the regulators took the position that the provincial privacy statutes, including BC PIPA, apply to any private sector organization that collects, uses and discloses information of individuals within the relevant province.[8] Their finding that the location of the data subjects was determinative appeared to suggest that the provincial privacy statutes have a broader reach than the federal privacy law, as the OPC and the courts have long recognized PIPEDA as applying only if the organization has a "real and substantial connection" to Canada.[9]

However, it does not appear that the OIPC asserted this broad jurisdictional claim to the Court on judicial review. Rather, the parties agreed that the "real and substantial connection" test is the appropriate test to determine whether provincial regulatory legislation is constitutionally applicable to out of province parties.[10] This approach effectively mirrors the one used by the OPC and the Federal Court when interpreting the application of PIPEDA.[11] Accordingly, it is now clear that the application of both federal and BC privacy laws requires a contextual analysis of the organization's connection to the relevant jurisdiction(s).

### Application of the Test to Clearview

The Court agreed with the OIPC that Clearview is subject to BC PIPA. The decision sets out a lengthy analysis whereby it notes that Clearview:[12]

- Provided its services to entities in BC, including BC law enforcement;
- Carried out business and marketing in BC; and
- Collected, used and disclosed information of individuals in BC.

Consideration of all these factors is consistent with the approach taken by courts and the OPC when assessing the jurisdictional application of PIPEDA to organizations outside Canada. However, the BC Court goes a step further. In obiter, the Court suggests that, even if Clearview did not market or provide its services in BC, the act of collecting, using and disclosing personal information of individuals in BC that is gathered from the Internet, alone, would create a sufficient connection to BC for BC PIPA to apply.[13]

The Court also found that the principles of order and fairness supported the application of BC PIPA to Clearview, given that:

- Privacy issues are increasingly cross-border in nature, and (similar to securities regulation), multi-jurisdictional regulatory authority "… promotes the seamless coverage of regulatory protection and the imposition of public interest remedies across the territories affected by a single, unlawful scheme";[14] and
- There is nothing unfair about BC PIPA applying to Clearview since it chose to enter the BC market, advertise its product to BC law enforcement agencies, and scrape data from the Internet that includes personal information of people in BC.[15]

Finally, it is worth noting that the Court in this case found that BC PIPA does not only apply to personal information about BC residents. Rather, the legislation regulates the conduct of organizations that collect personal information of persons with a direct link to BC, whether temporary or permanent. Accordingly, the OIPC was empowered to make orders with respect to personal information about individuals in BC regardless of whether those individuals are residents or temporary visitors in the province.[16]

## OTHER KEY FINDINGS

1. **Publicly Available Information**: The Court dismissed Clearview's claim that it did not require consent to collect, use and disclose the personal information that was scraped from public websites because such information was "publicly available." Although BC PIPA includes some exemptions to the statutory consent requirements for information available to the public from a prescribed source, the Court agreed with the OIPC that these exemptions should be interpreted narrowly. In particular, although consent is not required to collect, use and disclose "publications" that are available to the public (such as newspapers, books and

magazines) this exemption does **not** apply to all content that is posted on public blogs, public social media and other public websites.[17] Again, this finding is similar to the approach taken by the OPC and the courts when interpreting the "publicly available" exemption under PIPEDA.[18]

2. **Reasonable Purpose**: The Court upheld the OIPC's determination that Clearview lacked a "reasonable purpose" for collecting, using and disclosing personal information. In particular, the Court highlighted the risks of significant harm to individuals, including the potential for inaccurate facial recognition results and data breaches.[19]
3. **Order Validity**: The Court rejected Clearview's arguments that the OIPC's order was unnecessary, overly broad or unenforceable. The Court found the order to be necessary and consistent with BC PIPA's objectives of safeguarding personal information and protecting individual rights. It also found that Clearview was capable of making "best efforts" to cease collecting BC personal information and to delete previously collected BC data, based on representations Clearview had made in a separate court proceeding in Illinois.[20]

### Significance of the Ruling

This decision reinforces the existing case law that clearly indicates that privacy laws across Canada can apply to organizations outside the country or the relevant province. While this decision is not binding on courts or regulators in other provinces, it relies upon jurisprudence from the Supreme Court of Canada that would be equally applicable in other jurisdictions. Accordingly, there is a strong possibility that a similar analysis will be applied to evaluate the application of Alberta's *Personal Information Protection Act* and Quebec's *Act respecting the protection of personal information in the private sector*.

Organizations throughout Canada and worldwide should consider the application of the "real and substantial connection" test, and evaluate whether their activities are subject to, and compliant with, Canada's federal and provincial privacy statutes. In particular, organizations outside Canada should consider the broader regulatory and legal landscape that applies to facial recognition and data scraping technology, including the narrow definitions of "publicly available" personal information in relevant Canadian statutes. Failure to do so can result in significant costs and business impact, as demonstrated in this case where the Court upheld the OIPC's orders that effectively prohibit Clearview from offering its services in BC and require the company to undergo a potentially expensive process to geofence its data collection and purge BC data.

Clearview has filed paperwork to appeal this decision before the Court of Appeal for British Columbia, and it is therefore possible that we will see additional judicial guidance regarding the extraterritorial application of BC PIPA in the coming months.

[***Lyndsay A. Wasser*** l*eads McMillan's Privacy & Data Protection Group nationally. With nearly two decades of experience, Lyndsay advises on a wide spectrum of privacy and data protection matters, including valid consent protocols, data security, handling sensitive information, artificial intelligence, cross-border data transfers, data processing agreements, and privacy impact assessments. She co-wrote Privacy in the Workplace (3rd and 4th editions), is Co-Director of the Osgoode Certificate in Privacy and Cybersecurity Law, sits on Practical Law's US and Canada Advisory Board for its Data Privacy & Cybersecurity service, and has held the Certified Information Privacy Professional/Canada designation from the International Association of Privacy Professionals since 2013.*

***Kristen Pennington*** *(CIPP/C) is a Partner in the Privacy & Data Protection Group of McMillan LLP. Kristen counsels clients on the privacy law implications of new products, technologies, initiatives and corporate transactions, helps organizations develop privacy compliance programs, and drafts and negotiates privacy and data protection terms in an array of commercial agreements. Kristen was recently shortlisted for the Rising Star Award at the inaugural North American PICCASO Awards and was ranked by Chambers Canada as an Up and Coming lawyer in the area of Privacy & Data Protection.*

***Robbie Grant*** *is an Associate in McMillan LLP's Regulatory Group, with a focus on privacy and data protection matters. He frequently assists in drafting and reviewing privacy policies, responding to data breaches, and advising on the privacy law implications of various business practices and employment matters, including the use of artificial intelligence and employee monitoring.*]

---

1 *Clearview AI Inc. v. British Columbia (Information and Privacy Commissioner)*, [2024] B.C.J. No. 2354, 2024 BCSC 2311.

2 *Clearview v OIPC* at para. 90.

3 Clearview AI, "Overview", Clearview AI (date unknown) https://www.clearview.ai/overview

4 *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* (February 2021) at paras. 111 and 118.

5 *Clearview v OIPC* at para. 2.

6 OIPC, Order P21-08 (December 14, 2021).

7 *Clearview v OIPC* at para. 4.

8 *Joint Investigation Report* at para. 33.

9 *Joint Investigation Report* at para. 28.

10 *Clearview v OIPC* at paras. 70-75.

11 *A.T. v. Globe24h.com*, [2017] 4 F.C.R. 310, 2017 FC 114; *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427, 2004 SCC 45 at paras. 54–63 and the other authorities cited therein.

12 *Clearview v OIPC* at paras. 76 and 81.

13 *Clearview v OIPC* at paras. 90-102.

14 *Clearview v. OIPC* at para. 105, citing *Sharp v. Autorité des marchés financiers*, [2023] S.C.J. No. 29, 2023 SCC 29 at para. 134.

15 *Clearview v. OIPC* at para. 107.

16 *Clearview v. OIPC* at paras. 289-291.

17 *Clearview v OIPC* at paras. 164.

18 See, for example, *Joint Investigation Report* at para 45; *A.T. v. Globe24h.com*, [2017] 4 F.C.R. 310, 2017 FC 114 at para. 77.

19 *Clearview v OIPC* at para. 257.

20 *Clearview v OIPC* at paras. 267, 270-273, 279 and 292.