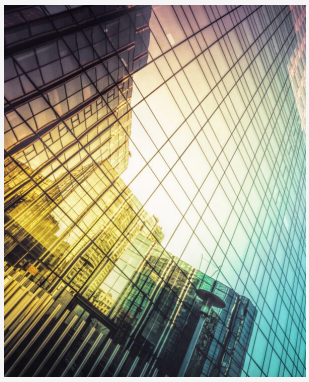
OSLER

Québec privacy commissioner continues to set high bar for biometric data processing: lessons for businesses

JANUARY 22, 2025 10 MIN READ



Related Expertise

- Artificial Intelligence
- Employment and Labour
- Privacy and Data Management

Authors: François Joli-Coeur, Joanna Fine, Gregory Corosky

At the end of last year, the oversight division of the Québec privacy commissioner, the Commission d'accès à l'information (the CAI), published its first decision since sweeping changes under Law 25 came into force. The decision (dated September 2024) resulted from a self-initiated investigation by the CAI into the biometric practices of a printing company that had made the CAI aware of its practices as required under Québec law. The CAI ordered the company to cease using facial recognition technology to control employee access to its premises and determined that the collection of facial biometric data was not sufficiently necessary or proportionate under the circumstances to justify the significant intrusion into employees' privacy that the practice allegedly constituted.

While consistent with the CAI's past orders and guidance, the decision highlights the high legal threshold for using facial recognition and other biometric identification technologies in Québec under the *Act respecting the protection of personal information in the private sector* (the *Québec Privacy Act*) and related provisions of the *Act to establish a legal framework for information technology* (the *Québec IT Act*).

The decision also reflects a trend in Québec over recent years where the CAI — empowered by the province's unique biometric filing requirements[1] — has taken enforcement action against companies that use these technologies and expressed skepticism about the necessity and proportionality of such tools. This trend is evident not only in the CAI's recent decision, but also in recent regulatory guidance[2], as well as the CAI's interactions with organizations that declare biometric systems.[3]

The CAI's position on the use of biometrics is particularly noteworthy for organizations, considering the significant financial penalties for non-compliance with Québec privacy laws. Under the *Québec Privacy Act*, administrative monetary penalties can reach up to $10 million or 2% of worldwide turnover, whichever is greater.

In this Update, we set out the key legal requirements for biometric identity verification systems in Québec, the CAI's application of these requirements to the facts in this decision, and key takeaways for businesses.

Legal framework and regulatory guidance

In Québec, private sector entities are subject to the *Québec Privacy Act*, which sets out the rules and principles governing their collection, use, communication and retention of personal information, including biometric data.

Biometric data is a sensitive category of personal information under the *Québec Privacy* Act[4] and the CAI has emphasized that its unique and immutable nature make it particularly sensitive.

Biometric data is also subject to unique biometric filing requirements in Québec. In addition to obtaining express consent, organizations must also declare their use of a biometric system for identification purposes to the CAI before its use, and must declare the creation of a biometric database to the CAI at least 60 days before deployment (a standard declaration form [PDF] is made available for this purpose on the CAI's website). When used for identification purposes, the CAI has consistently interpreted the biometric provisions of the *Québec IT Act* to require individuals to be provided with a non-biometric alternative to verify identity.

As highlighted in the CAI's guide on biometrics for organizations (available in French only), the *Québec Privacy Act* provides that the collection of personal information must be for a serious and legitimate reason, and be limited to only the information necessary for such purpose.[5] To assess compliance with these requirements, the CAI applies a two-pronged necessity test that requires organizations to demonstrate that the collection of personal information meets the following criteria

1. **legitimate, important and real objective**: the organization must establish that the objective pursued by the collection is legitimate, important and real
2. **proportionality**: the organization must establish that the invasion of privacy resulting from the collection is proportionate to the objective pursued, which in turn means demonstrating that
    - the collection is rationally connected to the stated objective
    - the invasion of privacy is minimized and
    - the collection is clearly more useful to the organization than harmful to the individuals concerned

In applying this test, organizations must consider factors such as the sensitivity of the personal information involved, the availability of alternative means to achieve the stated objective, and the consequences of the invasion of privacy for the individuals concerned. It is important to note that an individual's consent to the collection of their personal information is not sufficient to justify the collection if it does not meet the above criteria.[6]

Overview of decision

In this decision, an employer in the printing sector implemented a facial recognition system to control employee access to its premises. Initially introduced as a workplace health and safety measure to mitigate the spread of COVID-19, the employer continued to use the system for general access control after the height of the pandemic.

To verify identity using the biometric system, an employee would present herself or

himself in front of the biometric device at the entrance to the employer's premises. The system would then capture a photo of the employee's face and convert it into an irreversible numerical representation (also referred to as a "biometric template") to compare against the template created at the time of the employee's initial enrollment. If the templates were determined to be a match, access to the premises would be granted. While the system originally included a temperature check feature, this functionality was later discontinued and was not addressed in the CAI's decision.

Notably, the employer had obtained the consent of the employees to collect and process their biometric data and had declared the creation of a biometric database to the CAI, as required by law.

In applying the above-mentioned necessity test to the facts, the CAI concluded that the employer's collection of biometric data for access control purposes did not meet the requirements of the *Québec Privacy Act*.

Specifically, the employer failed the first prong of the test, as it could not demonstrate that its objective of using a facial recognition system for access control was "real" or "important," even though the security objective was itself considered "legitimate."

The CAI also found that the employer failed the second prong of the test. Although the collection was accepted as rationally connected to the objective, the CAI determined that the invasion of employee privacy was not sufficiently minimized, nor did the benefits of the system clearly outweigh the potential harms to employees.

As a result, the CAI concluded that the collection of facial biometric data contravened the *Québec Privacy Act* and ordered the employer to cease collecting facial biometric data, stop using the facial recognition system for access control purposes, and destroy all biometric data that had already been collected.

Takeaways for businesses

This decision illustrates the rigorous approach that the CAI takes when assessing the legality of collecting biometric data and other sensitive categories of personal information under the *Québec Privacy Act*. The decision may also have broader implications across Canada, given the heightened regulatory scrutiny surrounding facial recognition and similar technologies, as well as the ongoing public consultation initiated by the Office of the Privacy Commissioner of Canada with its *Draft Guidance for Processing Biometrics*.

While the CAI's conclusions in this decision are consistent with prior guidance and decisions, its analysis and application of each prong of the necessity test to the facts of the case provide valuable insights for organizations seeking to implement biometric identification solutions:

- **objective evidence of a real and important objective**: to demonstrate that a biometric system serves an important and real purpose, organizations must provide well-documented, objective evidence of a genuine issue or problem. Unless an organization operates in an industry or sector where heightened security or regulatory requirements mandate the use of biometric systems (e.g., critical infrastructure or highly sensitive environments), generalized allegations or speculative risks are typically insufficient. Companies should therefore carefully document the nature, severity and frequency of the problem that the biometric system is intended to address.

- **avoid general or convenience-based justifications**: operational challenges that are common to most organizations are unlikely to meet the "importance" criterion, as they are often seen as issues of convenience rather than necessity. Similarly, requirements in voluntary programs or certifications provide limited support, especially where biometric identification is optional or presented as one of several potential solutions rather than a mandatory requirement.
- **high threshold for proportionality**: the collection of biometric data represents a significant invasion of privacy due to the sensitive nature of the data, which stems from its intimate, unique and immutable characteristics. This high level of intrusion requires organizations to meet a commensurately high threshold to demonstrate proportionality.
- **security measures do not minimize privacy invasion**: while robust security measures, such as encryption, are important for protecting biometric data, they do not reduce the level of invasion of privacy inherent in the collection of such data. As a result, the implementation of strong security controls alone cannot justify the proportionality of the data collection.
- **consideration of alternatives**: organizations must provide documented evidence of the alternatives considered and explain why those alternatives were deemed insufficient to achieve the intended objective. For example, when biometric systems are used to control access to facilities, alternatives such as badges, cards, codes or keys typically should be considered. Claims that biometric solutions are more effective or that alternatives pose hypothetical risks (e.g., badge sharing or "buddy punching") are unlikely to be convincing unless supported by actual, documented evidence.

Key steps to compliance

To help mitigate regulatory risks and meet the high standards set by the CAI for lawful biometric data processing, businesses considering the implementation of biometric identification solutions in Québec should consider the following steps:

- **conducting a privacy impact assessment (PIA)** prior to implementing the biometric solution to assess and mitigate privacy risks and demonstrate compliance with all relevant privacy obligations (e.g., notice and transparency, valid consent, data minimization, retention and destruction, information security, cross-border data transfers and outsourcing, individual privacy rights) in the event of a complaint or inquiry. Note that under the *Québec Privacy Act*, an organization is required to conduct a PIA when acquiring, developing or overhauling a biometric system.[7]
- **assessing the necessity and proportionality of biometric data processing**, taking into account relevant regulatory guidance and decisions, including the above findings from the recent CAI decision (this evaluation should be documented in the above-noted PIA).
- **gathering relevant evidence, facts and statistics** to document and support your business case, including any claims regarding the necessity, proportionality, effectiveness and minimal intrusiveness of the proposed biometric solution.
- carefully preparing the biometric filing to the CAI, taking into account relevant legal and

regulatory obligations and working with relevant internal and external stakeholders (e.g., providers of biometric solutions) as necessary to ensure accuracy and completeness.

Additional details on the legal framework applicable to biometric data are available to AccessPrivacy subscribers, including in the Biometrics Topic Hubs. Visit AccessPrivacy to learn more.

---

[1] Sections 44-45, *Québec IT Act*.

[2] In its 2022 guide, "Biométrie : principes à respecter et obligations légales des organisations" [PDF] (available in French only), the CAI expressed concern about the growing reliance on biometric technologies and warned against trivializing their potentially significant privacy implications. Similarly, in a 2023 report, "Horodateurs et pointeuses biométriques – constats" (available in French only), the CAI concluded that most workplace biometric time clock systems it reviewed failed to meet the strict legal thresholds of necessity and proportionality under the *Québec Privacy Act*. This position is generally consistent with the CAI's previous decisions (see Auberge du lac Sacacomie inc., CAI 1014137-S, April 7, 2022; Enquête à l'égard de Compagnie Selenis Canada, CAI 1016217-S, January 14, 2022; Plainte à l'endroit du « Marché d'alimentation Marcanio et fils inc. »).

[3] In the context of biometric filings and other regulatory interactions, the CAI has demonstrated an increasing willingness to challenge the legality of biometric practices. Most notably, organizations that declare their use of a biometric system to the CAI often receive response letters regarding *potential* non-compliance. Although these letters do not constitute formal or binding decisions, they typically identify various *potential* violations based on the CAI's review of the submitted documentation and, in some cases, warn of potentially significant fines for failure to address these issues if a formal investigation is initiated.

[4] Section 12 para. 4(2) of the *Québec Privacy Act*.

[5] Sections 4 and 5 of the *Québec Privacy Act*.

[6] See para. 59 of the decision.

[7] Section 3.3, *Québec Privacy Act*.