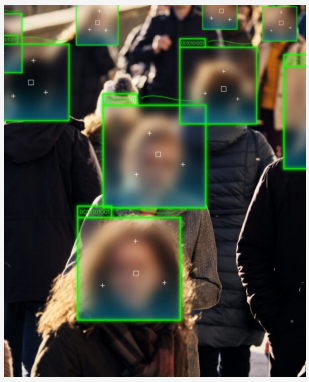
OSLER

Québec's privacy regulator prohibits retailer's use of facial recognition for loss prevention

MARCH 19, 2025 8 MIN READ



Related Expertise

- Privacy and Data Management
- Privacy and Data Security Disputes

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

On February 18, 2025, the Commission d'accès à l'information du Québec (the CAI) issued a decision prohibiting a major grocery and pharmacy chain from deploying its proposed facial recognition pilot project, which was aimed at preventing shoplifting and fraud in its stores.

While the use of video surveillance is a common practice in retail settings in Québec, this decision is an important reminder that the extraction of biometric data from raw video surveillance images must comply with stringent obligations under Québec's *Act to establish a legal framework for information technology* (the Québec IT Act) in addition to private sector privacy legislation.

The investigation specifically focused on assessing the company's compliance with the requirements set out in the Québec IT Act regarding the use of biometric data to verify or confirm identity. As a result, the decision did not address broader compliance issues under the *Act respecting the protection of personal information in the private sector* (the Québec Privacy Act), including whether the collection of biometric data using facial recognition met the necessity criteria in the particular context of the case,[1] and whether the collection would be for a "legitimate reason".[2] The necessity criteria was recently analyzed in another CAI decision involving the use of facial recognition technology to control employee access to the workplace (see our previous Osler Update, "Québec privacy commissioner continues to set high bar for biometric data processing: lessons for business," for details).

Summary of facts

Metro Inc., a major Canadian grocery and pharmacy retailer, planned to launch a pilot project in select locations to evaluate the feasibility of facial recognition technology as a loss prevention tool, with the potential for broader deployment. The project aimed to identify individuals previously involved in shoplifting or fraudulent activities at Metro stores. The CAI initiated its investigation shortly after the company declared its intent to create a biometric database, in accordance with Québec's biometric reporting requirements under section 45 of the Québec IT Act.

As part of the pilot, Metro would use its existing video surveillance system to capture facial images of suspected offenders and generate biometric templates to create a reference database. When a customer entered a participating store, the system would capture their

facial image, generate a new biometric template, and compare it against the stored templates to identify potential matches. If a match was found, designated store personnel would receive an alert to take appropriate action.

Québec's privacy legal framework

Companies in Québec that use biometric data to verify or confirm an individual's identity must comply with both the Québec Privacy Act, which sets out general requirements for the processing of personal information, and the Québec IT Act, which imposes specific legal obligations for biometric processing under sections 44-45.

Notably, the Québec IT Act imposes the following key legal requirements for the use of biometric data for identification purposes

- obtaining express (opt-in) consent from individuals before using their biometric data to verify or confirm their identity
- providing individuals with adequate notice of biometric processing and an alternative means of identity verification that does not involve biometric data
- declaring the use of biometric data for identification purposes, including the creation of a biometric database, within the prescribed timeframe set out in the Québec IT Act[3]

Failure to comply with these and other applicable legal requirements may result in regulatory enforcement actions, including orders to suspend, destroy or prohibit the deployment of a biometric database, or orders requiring modifications to biometric processing practices. In addition, under the Québec Privacy Act, certain violations may lead to fines or administrative monetary penalties, including penalties of up to $10 million or 2% of worldwide turnover for the preceding fiscal year, whichever is higher.

Key findings and conclusion

The CAI assessed whether Metro's proposed biometric process is subject to the Québec IT Act, and if so, whether its pilot project would ensure that express consent is obtained before biometric data is used to verify individuals' identities, as required by section 44 of the Act.

The CAI concluded that the company's pilot project would contravene the Québec IT Act by failing to obtain the required express consent. The CAI highlighted the automatic and systematic nature of the biometric data collection from all individuals entering the store and noted the company's own admission that it would not be possible to obtain express consent from each visitor.

In the absence of consent, the CAI held that the company's proposed biometric database constituted a significant "invasion of privacy" within the meaning of section 45 of the Québec IT Act, justifying the issuance of an order prohibiting the company from deploying the database in the present context. Notably, this is the first time that the CAI has relied on this statutory basis to issue such a prohibition.

Although the CAI readily concluded that express consent would not have been obtained in the context of the pilot project, the CAI's analysis of the company's arguments challenging the applicability of this requirement provides important clarifications on the scope of the biometric processing provisions of the Québec IT Act and their interaction with the Québec Privacy Act:

- **Scope of identity verification or confirmation under the Québec IT Act**: The company argued that its proposed use of biometric data for identification would not constitute "confirmation or verification" of identity under section 44 of the Québec IT Act. The CAI rejected this argument and adopted a broad, purposive interpretation of the provision. Specifically, the CAI clarified that identity verification and confirmation encompass both authentication (one-to-one matching) and identification (one-to-many matching) and do not require linking an individual to their name, date of birth, or other direct identifiers. As such, the company's proposed use of facial recognition to identify individuals involved in previous shoplifting or fraud incidents qualified as an identity verification process under the Québec IT Act.
- **Timing of biometric extraction and identification**: The company noted that the express consent requirement applies only when identity is verified "by means of" a process that captures[4] biometric data, which, in its view, means that the process must simultaneously collect biometric data and use it to verify an individual's identity. Since the project would have involved the collection and use of biometric data at different times, the company argued that the provision would not apply. The CAI rejected this argument, holding that the various stages involved in the identification process are interrelated and must be assessed holistically. Accordingly, the express consent requirement applies even if the collection of biometric data and the verification of identity would have occurred at different points in time.
- **Consent exceptions under the Québec Privacy Act**: The company also attempted to rely on the exceptions under section 12 of the Québec Privacy Act, which permit the use of personal information without consent for certain secondary purposes such as fraud prevention and detection, and for purposes consistent with the original purposes for which the information was collected. In concluding that the consent exceptions could not be relied upon for the pilot project, the CAI held that the extraction of biometric data from raw facial images in the video surveillance would constitute a new collection of personal information rather than a secondary use. As such, the company could not rely on the consent exceptions for secondary use of personal information to override the express consent requirement under the Québec IT Act when collecting biometric data to verify or confirm an individual's identity.

Key takeaways for businesses

While the use of video surveillance is a common practice in retail settings in Québec, this decision is an important reminder that the extraction of biometric data from raw video surveillance images must comply with strict legal requirements regarding the collection and use of biometric data for identity verification or confirmation.

In addition, businesses operating in Québec should be aware that the biometric-related requirements of the Québec IT Act, including the obligation to obtain express consent, take precedence over the Québec Privacy Act due to their more stringent nature. In addition, exceptions to consent for secondary purposes such as for fraud prevention or other legitimate business purposes are unlikely to apply when biometric data is used to verify or confirm identity.

Businesses considering the implementation of facial recognition or other biometric technologies should carefully consider their legal obligations under both statutes before deployment to ensure compliance and mitigate regulatory risk.

---

[1] In Québec, the "necessity criteria" refers to the obligations set out in sections 4–5 of the Québec Privacy Act, which require companies to limit their collection of personal information to what is necessary to achieve serious and legitimate purposes.

[2] On this point, the CAI references its Notice of Order to the company, which states that basing the proposed process on individuals who were involved in police interventions for shoplifting and fraud, rather than individuals who have in fact been found guilty, may violate the right to be presumed innocent and thereby impact the legitimacy test under s. 4 of the Québec Privacy Act.

[3] According to sections 44–45 of the IT Act, the declaration must be submitted to the CAI at least 60 days before the database is brought into service or, if no database is created, at any time before the biometric data is used for identification purposes.

[4] The decision did not specifically address a discrepancy between the English and French versions of section 44 of the Québec IT Act. The French version uses the term "saisir" (roughly translating to "capture") to describe the biometric process covered by this provision, suggesting a focus on the collection stage. In contrast, the English version emphasizes the subsequent use of biometric data, referring to "a process that allows biometric characteristics or measurements to then be used." Although this discrepancy was not specifically discussed, it further supports the CAI's conclusion that the various stages of biometric processing must be assessed holistically when determining whether section 44 applies.