APRIL 8, 2025 • 7 MIN READ

Québec's Commission de l'accès à l'information adopts a broad and liberal interpretation of privacy legislation respecting biometric information

AUTHORS

 Julie Himo

 Rosalie Jetté

 Krystelle Metras

In a recent decision, the Commission d'accès à l'information (the CAI) rejected a facial recognition project planned by Metro Inc. (Metro) by concluding that it is illegal under the *Act to establish a legal framework for information technology* (the AELFIT).

The main issue was whether the facial recognition project was subject to section 44 of the AELFIT.

What you need to know

- Metro was planning a facial recognition project to identify any individuals who have been involved in shoplifting or fraud in its establishments.
- The CAI determined that the proposed project required the express consent of the individuals whose images would be captured, and failure to obtain such consent constitutes an invasion of privacy.

Background

The proposed facial recognition project

In September 2024, Metro advised the CAI that it intended to set up a database of biometric characteristics or measurements to support the implementation of facial recognition systems in some of its establishments, with the aim of curbing shoplifting and fraud. The facial recognition would be based on images captured by surveillance cameras set up at the entrances and exits of its establishments, which an algorithm would compare against a database of images captured by surveillance cameras during shoplifting or fraud incidents involving adult individuals that required law enforcement measures. In the event of a match between the image captured by the surveillance camera and the database, the establishment's management would be alerted.

CAI's investigation and notice

In October 2024, the CAI's oversight division notified Metro that its proposed facial recognition project raised concerns about the application of the *Private Sector Act* and the AELFIT. In his preliminary report, the investigator noted, among other things, that Metro did not plan to obtain the express consent of the individuals concerned by the

creation of the database and the facial recognition process.

In November 2024, the CAI issued a notice advising Metro that the first phase of the investigation showed that its project could violate the privacy of the concerned individuals by failing to obtain the express consent required under section 44 of the AELFIT.

Metro's comments

Metro claimed that section 44 of the AELFIT did not apply in this case because the proposed process did not involve verifying or confirming a person's identity and, therefore, the express consent of the concerned individuals was not required.

Metro asked the CAI to adopt a strict interpretation of identity verification or confirmation under section 44 of the AELFIT, arguing that identifying a person by using biometric characteristics or measurements does not constitute identity verification or confirmation under section 44.

Metro also argued that section 44 did not apply to its project since the three elements of section 44 (i.e., verification or confirmation of identity, using a process that captures biometric characteristics or measurements) would not occur simultaneously during the proposed facial recognition process.

CAI's decision

After establishing that Metro was subject to the *Private Sector Act* [translation] "with respect to the information it collects, retains, uses or discloses to third parties" because it operates a business in Québec, the CAI confirmed that section 44 of the AELFIT applied to Metro's facial recognition project and that, as such, Metro needed to obtain the express consent of the individuals concerned by the facial recognition process.

According to the CAI, the creation of a biometrics database, as well as the requirement to verify a person's identity by means of a process that captures biometric characteristics or measurements without obtaining their express consent, as required by section 44 of the AELFIT, constitute an invasion of privacy.

Capturing biometric characteristics or measurements

After analyzing the proposed process of capturing images and converting them into digital representations, the CAI concluded that "the images captured by video surveillance and fed to the database constitute biometric characteristics, and the digital representations of these images produced by each of the projected systems constitute biometric measures, within the meaning of section 44 of the AELFIT"[1].

Verifying or confirming a person's identity

The CAI points out that privacy laws have quasi-constitutional status in Canada.

Since personal information of a biometric nature is considered sensitive information, the legislator provided for the obligation to obtain the express consent of individuals when "it is required that their identity be verified or confirmed using this information"[2].

Analyzing and interpreting the legislator's intent, the CAI concluded that section 44 of the AELFIT should be given a broad and liberal interpretation in order to achieve its essential objective, namely the protection of biometric personal information.

Consequently, since the biometric information of people who enter a Metro establishment is part of a system that recognizes individuals and distinguishes them from one another, Metro's facial recognition system allows "a person's identity to be verified or confirmed" under section 44 of the AELFIT.

The CAI also determined that the various steps required in the facial recognition process do not have to be carried out simultaneously, contrary to Metro's arguments. The whole process must be taken into consideration based on the

broad and liberal interpretation applied to section 44 of the AELFIT.

Requiring facial recognition without prior consent constitutes an invasion of privacy

Since any person entering a Metro establishment would have their identity automatically verified, the CAI ruled that the "facial recognition process constitutes an actual requirement, because no one can enter the establishment without their biometric characteristics or measurements being collected and compared with those contained in the [Metro] database"[3].

The CAI also pointed out that Metro did not plan any means for obtaining the express consent of individuals affected by the facial recognition process. Metro considered that obtaining this consent was impossible.

According to the CAI, the creation of a biometrics database, as well as the requirement to verify a person's identity by means of a process that captures biometric characteristics or measurements without obtaining the express consent required by the AELFIT, constitutes an important violation of privacy.

Practical considerations for companies

As companies increasingly turn to processes that use biometric information to ensure the safety of their operations, the CAI's decision regarding Metro's practices reinforces the trend towards a broad and liberal interpretation of the AELFIT's provisions imposing limits and requirements on the use of biometric information.

For this reason, companies wishing to use processes involving the collection and use of biometric information should consider adopting the following risk mitigation measures:

- Anticipate the time required to file the necessary declarations with regulatory authorities, such as the CAI in Québec, when planning the implementation process.
- Document any analysis of privacy issues, and specifically any data justifying the measure chosen or the absence of an alternative to a process that uses biometric information. This supporting data should clearly indicate the actual (and not hypothetical or anticipated) reasons why such a measure is required (e.g., the need to regularly process sensitive information, frequent wrongdoing incidents, or a lack of effective alternative measures).
- Disclose to the affected individuals, by any conceivable means, the existence of a process that uses biometric information (signage at the entrance, notice on the company's website, etc.) and consider any method for obtaining their express consent.
- Review data protection and retention policies to ensure that data is destroyed once its purposes have been fulfilled and that it is safeguarded according to its degree of sensitivity in the relevant systems (e.g., asset protection and monitoring infrastructure and tools, data encryption, and least privilege access control).

FOOTNOTES

To discuss these issues, please contact the author(s).