JANUARY 30, 2025 • 6 MIN READ

Transcontinental Printing Inc.: Québec's Commission d'accès à l'information orders the company to stop collecting its employees' biometric data

AUTHORS

 Julie Himo

 Rosalie Jetté

 Roxanne Beaucage

In a recent decision, Québec's Commission d'accès à l'information (CAI) concluded that Transcontinental Printing Inc. (Transcontinental) had collected the biometric data of its employees in violation of the *Act respecting the protection of personal information in the private sector* (Private Sector Act). Transcontinental failed to demonstrate the necessity of the personal information it was collecting in order to ensure the safety of its employees and its premises, and to comply with the Customs-Trade Partnership Against Terrorism (CTPAT) certification standards.

This is the CAI's 10th decision on biometrics since 2000, which makes it all the more relevant in a context where the creation of biometric data banks is rapidly growing in Québec.

What you need to know

- **Obtaining prior consent for the collection of personal information does not constitute an exemption from the requirements of the Private Sector Act.** Under the Private Sector Act, organizations must ensure that they are collecting data for predetermined, serious and legitimate purposes, and that the collection is necessary. Obtaining employees' consent to the collection of their personal information cannot be relied on as an exemption from the requirements set out in the Private Sector Act.
- **Biometric data is considered sensitive personal information that entails a high level of reasonable expectation of privacy.** The CAI distinguishes biometric personal information from other traditionally collected information, such as unique identifiers linked to cards or passwords, since biometric data cannot be easily replaced in the event of a privacy incident given its permanent and distinctive nature.
- **Organizations must evaluate the possibility of using other, less intrusive means to achieve their stated purpose.** Organizations collecting personal information have a duty to minimize the invasion of data subjects' privacy.
- **Organizations cannot rely on specific industry standards to argue that the purpose of the collection is real**. Although useful in demonstrating the legitimacy of the purpose, industry standards voluntarily followed by an organization cannot be relied on to demonstrate that the purpose is real. Organizations must be able to demonstrate that the collection addresses a real and specific problem affecting their activities.

Background

During the Covid-19 pandemic, Transcontinental, a printing company, implemented a dual-function authentication system featuring facial recognition and body temperature measurement. The company's objective was 1) to ensure the safety of its employees and premises by limiting the spread of the virus; and 2) to comply with CTPAT certification requirements. In 2023, Transcontinental stopped taking the temperature of its employees and destroyed the data that it had collected. However, the company continued to collect biometric data through its facial recognition system.

Decision

The CAI concluded that Transcontinental breached the Private Sector Act by using a facial recognition system to collect biometric personal information in order to control access to its premises, ensure the security of its employees and, incidentally, meet CTPAT certification requirements.

The purpose of the collection must be legitimate, important and real

Although the CAI agreed that protecting and managing access to its premises was a legitimate purpose, it concluded that Transcontinental had not demonstrated that this purpose was real in the specific context of the company. The use of biometric data was not supported by specific or problematic events that justified the need for collection. In addition, the company did not present any evidence of an existing issue with managing access to its premises, so that the risk was only hypothetical. According to the CAI, controlling access to an organization's premises is a typical management objective, and is not sufficiently important to justify the collection of sensitive personal information. The CAI indicated, however, that a higher level of security may be required for organizations in some industries, which could justify the use of biometric measures in certain cases. However, the CAI ruled that the printing industry did not require a sufficient level of security to justify the use of facial recognition to achieve the objectives alleged by the company.

As for Transcontinental's argument that the CTPAT certification requirements justified the purpose of the collection, the CAI disagreed, stating that the use of authentication systems based on biometric data is not a requirement but rather a suggested means of ensuring the premises' physical security. As noted by the CAI, CTPAT standards themselves provide for other, less privacy-intrusive means of achieving Transcontinental's objectives. Finally, CTPAT certification is voluntary, so it cannot be relied on as an exemption from an organization's legal obligations.

The privacy intrusion must be proportional to the purpose

Given the high level of reasonable expectation of privacy with respect to biometric data, the CAI ruled that the collection of Transcontinental employees' biometric data was not proportional to Transcontinental's purpose, particularly given the existence of much less intrusive means that would limit the intrusion of the employees' privacy and still achieve Transcontinental's purpose. The CAI also concluded that the harm resulting from the collection far outweighed the useful effects to the company since, even though facial recognition can be an effective means, Transcontinental had not demonstrated how this method provided superior benefits that would justify the harm for its employees.

Impact on business conduct

The Transcontinental case is a reminder for organizations to be vigilant when they intend to collect sensitive personal information. They should consider the use of alternative, less intrusive means of achieving their objectives, before resorting to biometric data collection tools. If they wish to use a system requiring the collection of sensitive information, such as biometric data, organizations should document 1) the purposes for which the information is to be collected; 2) the reasons why these purposes are real and important for the organization, namely that they address

a real and specific problem and not a hypothetical risk; and 3) the assessment of other means that were considered to achieve the same purpose and the reasons why alternative solutions were discarded or were considered inadequate to meet the intended purpose.

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