# Transparency – Identification, Location or Profiling Technologies (ss.81., 8.2)

Quebec's Private Sector Privacy Law Amendments C. 25

## Introduction

On September 22, 2021, Quebec passed *An Act to modernize legislative provisions as regards the protection of personal information* (2021, c. 25) (the Act) updating public and private sector privacy laws. The provisions of the Act come into force over a period of 3 years.

This document was created by leading Canadian privacy experts working with national and regional industry associations. We believe a harmonized approach to privacy law across Canadian jurisdictions is important so that the rules are understandable for individuals and enterprises. Interpretations of privacy laws should be pragmatic, reasonable and focus on the privacy outcomes for individuals and operationalization expectations for enterprises. With this in mind, we have created what we think is appropriate guidance for interpreting some of the more challenging provisions of the Act.

This document can be shared and used by enterprises. This is not legal advice; it is suggested best practices for entities wishing to work pragmatically on their compliance with the Act before any additional guidance from the *Commission d'accès à l'information* (the "CAI") or regulations are made available. We encourage enterprises to monitor developments in CAI and government guidance on these and other topics related to the Act.

## Transparency – Identification, Location or Profiling Technologies

When an organization uses personal information for profiling, location and/or identification technologies, the law includes new disclosure requirements intended to enhance transparency for individuals.

Section 8.1 states that:

- Organizations must inform individuals of any collection of personal information using a technology that includes functions allowing the individual to be identified, located or profiled.
- Organizations must also inform individuals of the means available to activate such functions.
- "Profiling" is defined as the "collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person's work performance, economic situation, health, personal preferences, interests or behaviour".

- The terms “identify” and “locate” are not explicitly defined in the Act; however, these terms might be reasonably defined as follows:

    - “identify” means to associate anonymous or pseudonymous data with a specific natural person

    - “locate” means to determine the geographic location of a natural person with reasonable accuracy, such as identifying longitude/latitude coordinates, or determining a user is located within a city block. In the normal course, “locate” would not include inferring that a user is located in a particular country or municipal area, which may be inferred through IP address/Internet Service Provider

Below is a breakdown of the new requirements along with recommended guidance:

**1. Using personal information for identification, location and profiling technologies**

An organization that collects personal information using technology that identifies, locates or profiles an individual must inform the individual of the use of such technology and the means available to activate it.

If you answer yes to the following questions, then you have an obligation to inform.

**a. Are you using technology that identifies, locates or profiles an individual?**

- **Identification of an individual:** Are you using technology that permits an individual to be identified (not in a pseudonymous way, but as a natural or identifiable person)? **Location of an individual:** Are you tracking the geographic location of an individual (i.e. where they are or where they have recently been)?

    - Consider accuracy and precision. Rather than inferred location, are you attempting to accurately identify an individual’s “true location” rather than their imprecise location (e.g a city or country)?

- **Profiling of an individual:** Are you analyzing or predicting an individual’s characteristics or behaviour based on personal information?

    - The law has a very broad definition of 'profiling', which encompasses any personal information processing made to assess characteristics of an individual in any contexts and for any purposes – both offline and offline.

    - Most often, profiling is intended to better reach and serve customers, including to:

- Serve more relevant and targeted advertising or price products or services based on inferred interests, reliability, behaviour or location.
- Suggest more relevant products based on an individual's purchase history, economic situation, preferences or interests.

The obligation to inform is not just in relation to potential and current customers, but to any individual who interacts with your organization, including website visitors and employees.

When the collection of personal information is on behalf of a third party, it is the final user who must ensure compliance with all requirements under the law.

**b. Are you using personal information?**

The requirements extend to the use of personal information, but do not apply to the processing of anonymous or aggregate information.

**2. Obligation to inform individuals**

Once you confirm that your organization is collecting personal information using a technology that includes functions allowing an individual to be identified, located or profiled, there is a new obligation to inform the individual.

**a. How and what to inform**

- Organizations should be upfront and as transparent as practicable using plain language.
- Informing can take place through various means and organizations can take a multi-layered approach, as appropriate and reasonable (e.g. general information in a privacy policy, terms and conditions, website, FAQs, and more specific information on forms or in other direct communications like a "just in time" notice or pop up).
- Notification should always be reasonably prominent. The level of prominence and detail should depend on the circumstances, including the following factors:
    - The impact of the identification, location or profiling on the consumer.
    - The reasonable expectations of the individual; the more unexpected an activity may be, the more steps an organization should take to bring it to an individual's attention.

- [Associations to include sector, industry or profession-specific examples as appropriate]

- Be clear with customers about which functions are activated by default (i.e. "By downloading this app, you are going to be profiled, which means…."). See section 3 below.

- Organizations should also consider cases where an opt-in may be appropriate. See section 4 below.

**b. When to inform**

- Depending on the circumstances, organizations should inform individuals at the time of collection of the personal information.

**3. Inform individuals of the means to activate functions**

Organizations must provide notice to individuals of those circumstances where there is, in fact, a process for an individual to activate the functions described above (i.e. functions that enable a person to be identified, located, or profiled).

In addition to being clear with customers about which functions are activated by default, organizations must be clear about the choices individuals have to expressly opt in to features in accordance with their preferences.

- Organizations should consider providing options to activate functions that would optimize performance and personalization, rather than functions that are necessary to deliver a product or service.

    - E.g. A dating website or app could give users the option of turning on location tracking to enhance an individual's experience by showing other users nearby. The feature would optimize, rather than be critical to, the delivery of the overall service.

**4. Consider cases where an opt-in is appropriate**

On a case-by-case basis, organizations should consider when express consent may be appropriate. See separate guidance on consent.

Organizations should make a contextual assessment of the reasonable expectations of individuals, as well as any risk of harm to the individual, in determining whether consent should be required (or whether an exception to consent applies).

- Consider an individual's reasonable expectations: E.g. Given what could be real safety issues, opt-in might be required for precise location tracking in the context of

social media applications. There should also be opt-in for any location tracking when an app is not being actively used.

- Identification and profiling should require opt-in for any activity that might be associated with or reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, state of health or sex life or sexual orientation.

When personal information is sensitive (Section 12, subsection 4), as well as when medical, biometric or “otherwise intimate information” is used, express consent is a requirement (e.g. using a fingerprint or facial image, or tracking a person's heart rate). Some types of profiling are already subject to separate regulatory restrictions (e.g. consumer credit reporting), which override any guidance given.