Confidentiality Default Settings

Quebec's Private Sector Privacy Law Amendments C. 25
Section 9.1

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 practical implementation 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.

Confidentiality Default Settings (s.9.1)

The confidentiality default setting requirements apply only if an individual or enterprise:

- Offers a technological product or service to the public; and
- The technological product or service collects personal information; and
- The technological product or service has privacy settings that are adjustable by the individual; and
- The adjustable privacy settings are not browser cookies (browser cookies are exempt from s.9.1).

If all the above criteria are met, the privacy settings of the technological product or service must be set, by default, at the highest level of confidentiality that is reasonable based on:

i. the core functionality of the service; and

ii. the individual's reasonable expectation in light of the core functionality of the product or service and any accompanying notice.

Key terms in the section are not defined: "*technological product or service*", "*privacy settings*" and "*the highest level of confidentiality by default*". These terms should be interpreted as conforming with the reasonable expectations of the individual and being compatible with the core functionality of the product or service. The section should not be intended to make technological products and services impractical for individuals to use.

"*technological product or service*"

"Technological" designates a subset of all products and services, applying broadly to digital products and services, such as mobile applications, online social media networks, networked remote monitors (digital health and fitness monitors, vehicle use monitors, smart homes), networked appliances, digital recording devices, etc.

"*privacy settings*"

"Privacy settings" means the parameters in the technological product or service that relate directly to privacy and can be changed by the individual user through a user interface.

> Ex.: It may be reasonable for a route finding app to collect an individual's location when the app is on and route queries are being made, with notice. It may not be reasonable for an app to collect an individual's location all the time, without express consent.

"*the highest level of confidentiality by default*"

The requirement to have privacy settings at "the highest level of confidentiality by default" should rely on context and align with a user's reasonable expectations.

Transparency, primarily in the form of notice, is a key factor influencing an individual's reasonable expectations. The user's reasonable expectations are also shaped by:

- the core functionality of the technological product or service; and
- the sensitivity of personal information involved.

When the collection of personal information is reasonably required for the operation of core functionalities (e.g. basic service provision, billing, security, fraud prevention and operational diagnostics for the product or service), the default privacy setting should be set as "active".

The default privacy settings related to unexpected or non-core functionality should be set as "inactive" and only activated by the individual after a proper notice has been made available. The objective is to prevent the unexpected or unreasonable collection, use or disclosure of personal information through technological means.