New Québec biometric requirements: legal risk and mitigation

April 20, 2022

Biometric technologies are increasingly becoming part of our lives due to the widespread usage of smartphones, e-passports and digital ID cards. Generally used to enhance security, these technologies raise important privacy issues, particularly with respect to the inherent sensitivity of the biometric information.

In 2001, Québec was the first jurisdiction in Canada to introduce the *Act to establish a legal framework for information technology* (QC IT Act), which includes specific provisions regulating the use of biometric databases to ensure that they are managed with an adequate level of protection. For instance, organizations are required to report the use of any database containing biometric characteristics or measurements (or "biometric information"). Once in force in September 2022, the *Act to modernize legislative provisions as regards the protection of personal information* (QC Bill 64), which amended the QC IT Act, will impose two new requirements pertaining to the reporting (that is, "declaration" or "disclosure") of biometric systems used for identification or authentication purposes**.** In fact, in addition to the existing requirement to obtain the express consent from individuals for the collection of their biometric information, organizations will be required to disclose any process involving biometric information, regardless of whether biometric information is stored in a database. Otherwise, organizations will not be permitted to use biometric information for the purposes mentioned above.

Before tackling these new obligations, we find it useful to recall certain key concepts regarding biometrics and the protection of biometric information.

Key concepts

Biometrics (which literally means "measurement of the human body", in Greek) is a technology that allows the mathematical analysis of a person's biological, morphological or behavioral characteristics. When we discuss biometrics under the QC IT Act, we refer to systems used to identify or confirm the identity of individuals by using their biometric information, such as fingerprints, iris and retina prints, hand and face geometry, or voiceprints. This is an important point given that biometric information is considered sensitive personal information and thus, it is subject to public/private sectors data protection laws regardless of the purpose of its use.

Identification and authentication are the two main functions of biometrics. Their technical operation is different, which may lead to distinct legal implications and risks. While the notion of “identification” means to find an identity in a database to determine who the person is, the notion of “authentication” instead consists of verifying or confirming the identity of an individual. For example, identification may be used to authorize or deny access (that is, the captured biometric information was found in a database), whereas authentication allows to verify or confirm if the individual is who he claims to be. The identification function will generally trigger more risks since a biometric database must be implemented, which is not necessarily the case for the authentication function.

Now, let's take a look at the amendments made to sections 44 and 45 of the QC IT Act by QC Bill 64.

Bill 64 amendment to section 44, QC IT Act

According to the wording of QC Bill 64, section 44 of the QC IT Act is amended as follows (changes in red below):

> **Section 44**. A person’s identity may not be verified or confirmed by means of a process that allows biometric characteristics or measurements to be recorded, ~~except with the express consent of the person concerned. Where consent is obtained, only~~ except where such verification or confirmation has been previously disclosed to the Commission d’accès à l’information and except with the express consent of the person concerned. Only the minimum number of characteristics or measurements needed to link the person to an act and only such characteristics or measurements as may not ~~be recorded~~ then be used without the person’s knowledge may be recorded for identification purposes. No other information revealed by the characteristics or measurements recorded may be used as a basis for a decision concerning the person or for any other purpose whatsoever.
>
> Such information may only be disclosed to the person concerned, at the person’s request. The record of the characteristics or measurements and any notation relating thereto must be destroyed as soon as the purpose of verification or confirmation of identity has been met or the reason for the verification or confirmation no longer exists.

Under this section, an organization is required to obtain the express consent (opt-in) of individuals to identify/authenticate them using their biometric information. Therefore, organizations should provide an alternative method of identification/authentication for individuals who do not provide their consent. In addition, individuals must be properly informed (usually via a privacy notice and a consent form) about the nature, purposes and consequences of the processing of their biometric information, which must also meet the reasonable purpose standard, regardless of whether express consent was obtained. The recent amendments have not modified this requirement.

The first edit of this amendment provides that, in addition to the express consent of the individual, any process used to verify or confirm the identity of an individual using their biometric information must be reported beforehand to the Commission d’accès à l’information (CAI). In other words, this obligation now **extends to any use of biometric information to identify or confirm a person ’s identity regardless of whether a database is created** , which aligns with the CAI’s recommendations regarding QC Bill 64

in its position paper titled « Mémoire de la Commission d'accès à l'information présenté à la Commission des institutions dans le cadre des consultations particulières et *auditions publiques* ». While no clear formality has been set by the Québec legislator in relation to this new obligation (*i.e.* a form to use for the reporting, a timeline, etc.), the CAI may publish guidance by the time this amendment comes into force.

As for the second edit of section 44, a comparative analysis between the English and French versions of this section is necessary to understand what it means. Since its enactment in 2001, the QC IT Act, which is drafted differently than most laws and includes new concepts, has triggered much uncertainty and also caused several interpretation issues. The replacement of the terms "be recorded" by "then be used" by QC Bill 64 does not in fact provide more clarity. However, we understand that the biometric information collected should be minimal and only be "used" (instead of "recorded") if the individual is aware of it. This is consistent with the original language provided in the French version of this section and with the first edit of the amendment that extends the scope of this section to any use of biometric information.

Bill 64 amendment to section 45, QC IT Act

According to the wording of QC Bill 64, section 45 of the QC IT Act is amended as follows (changes in red below):

> **Section 45.** The creation of a database of biometric characteristics and measurements must be disclosed beforehand to the Commission d'accès à l'information in a timely manner no later than 60 days before it is put into use. ~~The creation of a database of biometric characteristics and measurements must be disclosed beforehand to the Commission d'accès à l'information. As well, the existence of such a database, whether or not it is in service, must be disclosed to the Commission.~~
>
> The Commission may make orders determining how such databases are to be set up, used, consulted, released and retained, and how measurements or characteristics recorded for personal identification purposes are to be archived or destroyed.
>
> The Commission may also suspend or prohibit the bringing into service or order the destruction of such a database, if the database is not in compliance with the orders of the Commission or otherwise constitutes an invasion of privacy.

This amendment provides that the creation of a biometric database must be reported to the CAI no later than 60 days before the database is put into effect. In other words, organizations will have to disclose their intention to implement a biometric database at least two months before it is actually implemented. This reporting requirement must respect the formalities required by the CAI (that is, reporting the database using the required form). It is worth mentioning that while the CAI has broad powers in relation to biometric databases (such as the power to make orders pertaining to the management, implementation and destruction of such databases, as well as the archiving and destruction of measurements or characteristics, as more fully described in section 45), the CAI will not have these same powers over organizations using biometric technologies that do not store biometric information in a database.

Legal risk and mitigation strategy

When assessing the level of privacy risk that arises from the processing of biometric information, organizations may consider the following factors:

i. whether the technology is intrusive in terms of privacy or physical integrity;
ii. what is the purpose for which it is used;
iii. whether it is possible to use another process to achieve the same objectives; and
iv. how the biometric information is managed, stored and destroyed.

The degree of invasion of a person's physical integrity or privacy usually depends on the biometric characteristic captured, which is inherent to the human body and can reveal much more personal information than the characteristic itself. For example, iris and retinal scans are generally considered more intrusive than voice ID systems, because of the light beams that touch and penetrate the eye. A retina may also reveal several types of medical conditions, such as AIDS, syphilis, leukemia, lymphoma, and congestive heart failure. Furthermore, other related risks should also be assessed, such as the circulation of biometric information, increased surveillance, misuse or identity theft.

To mitigate legal risks, organizations should consider establishing guidelines for the use of biometric systems providing for the above obligations and other applicable principles governing the protection of biometric information. Organizations should also consider conducting a privacy impact assessment (PIA) prior to deploying a biometric technology. This will help identify legal risks, as well as controls that should be implemented to mitigate these risks. Such controls may include reducing the amount of information being collected, providing a more prominent notice to individuals concerned, encrypting data in transit and at rest, or limiting the retention period, for instance. In this sense, a PIA is an organization’s roadmap for implementing a privacy-protective solution and can help demonstrate to privacy regulators that the organization has done its homework.

Finally, we note that once QC Bill 64 is in force, a privacy impact assessment will become mandatory for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the processing of personal information in the private and public sectors. In this regard, BLG’s Compliance Guide provides an overview of the Québec Privacy Law Reform and a perspective on what steps should be taken to comply with the new requirements.

Expertise

Corporate Commercial, Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749