Biometrics in Québec:
Application Principles

Making an Informed Choice

Commission d'accès à l'information
July 2002

Presentation

This document provides information on biometrics application principles in the province of Québec. The principles are derived from an initial examination of the *Act respecting Access to documents held by public bodies and the Protection of personal information* (R.S.Q., c. A-2.1) (the "Act respecting Access"), the *Act respecting the protection of personal information in the private sector* (R.S.Q., c. P-39.1) (the "Act respecting the private sector") and the *Act to establish a legal framework for information technology* (R.S.Q., c. C-1.1) (the "Act respecting information technology").

The application principles are neither limitative nor exhaustive and have been issued for the sole purpose of helping you make an informed choice.

If you are planning to use biometrics in your organization, the series of questions below will guide you in assessing whether your project is in compliance with the laws.

- **Application Principles**

Principle 1
Alternatives to Biometrics

The Act respecting information technologies states that a person's identity may not be verified or confirmed by means of biometrics, except with the express consent of the person concerned.

Have you considered an alternative to biometrics?

What alternative to biometrics is available to persons who wish to use this type of technology?

How do you provide for the exercise of a person's free choice not to use biometrics in the workplace?

Principle 2
Necessity of Information Collected

Any public body wishing to use biometrics must ensure that the personal biometric data and other personal information collected are necessary for the carry out the attributions of the body or to implement a program under its management. In the private sector, the information collected must be necessary for the object of the file established.

Necessity means that the information collected is indispensable. The obtainment of consent to collection is subject to this requirement of necessity.

In addition to necessity, the Act respecting information technology states that only the minimum number of characteristics or measurements needed to link the person to an act may be recorded.

Can the necessity of the data collection you are planning be demonstrated? How?

Can the purposes sought by the collection be attained without such information?

How do you ensure that only the minimum amount of biometric information is collected?

Have you thoroughly analyzed the risks inherent in the technology you plan to use and the risks associated with the use you wish to make of the technology? For the enterprise or body wishing to install the technology? For future users of the same technology? For example, if you have decided to collect fingerprints, have you taken into account the specific risks that this technology presents with respect for privacy?

What reasons warrant the collection of personal information?

Is other personal information being collected for the same purpose?

Principle 3
Collection From the Person Concerned

The Act respecting information technology states that biometric characteristics or measures shall not be recorded without the knowledge of the person concerned. Biometric data may therefore not be collected without the knowledge of that person.

How do you ensure that data are collected directly from the person concerned?

How do you validate the identity of the person when the biometric data are collected?

How do you ensure that the person concerned is fully aware that biometric data are being collected about him or her, and what are these data when the identity is verified? ... subsequently when the person's identity is confirmed?

Principle 4
Consent to the Use of Biometrics

The Act respecting information technology requires a person's express consent to have his or her identity verified or confirmed by means of a process that allows biometric characteristics or measurements to be recorded. The express consent must pertain only to the collection of biometric data and must be in writing, given freely in an informed manner, specific, and limited in time.

Considering the risks related to the use of biometrics (for example: permanent identity theft, centralized database security, network security, personal discrimination, technology piracy, limits of the technology used, etc.), what form of consent will you require of the persons concerned?

Do you validate the identity of the person whose consent you are seeking? How?

Do you ensure that the consent sought meets the requirements described above? How?

Do you inform the person concerned of all known risks associated with or inherent in the biometric system and technology used in order that such person may give his or her informed consent? How?

What mechanism have you planned on implementing to prevent persons who refuse the use of biometrics from feeling pressured or inconvenienced?

Do you inform the person of the duration of retention and the time of destruction of the biometric characteristics or measures collected? How?

Do you describe all the measures and characteristics recorded as well as any other information that may be revealed by such measures and characteristics to the person concerned? How?

Principle 5
Retention and Use of Biometric Data

Considering the risks entailed in the collection of biometric data, numerous precautions must be taken. Specific conditions apply to the storage of this type of sensitive information, which requires particular attention and adapted security measures. The Commission considers that all biometric and associated data must be encrypted.

The creation of a database of biometric characteristics and measurements pursuant to the Act respecting information technology and, as the case

may be, the Act respecting Access shall be disclosed beforehand to the Commission d'accès à l'information.

Have you opted for solutions in which the user's biometric measures are held on a portable medium (encrypted and secure) under the user's control?

If you wish to create a biometric database, have you disclosed your intention to the Commission d'accès à l'information? Have you also disclosed the existence of such a database, whether or not it is in service?

In creating a database, have you planned to encrypt all data contained in or linked to such a database during its retention? When making back-up copies and for relief purposes? When such data is circulated or passes through a network (or several networks), whether the network is public or private and internal or external?

What other security measures will be used to protect the biometric data and ensure its security and confidentiality?

Is the degree of security afforded by the use of biometrics proportionate to the requirements of the purposes sought?

Do you ensure that the biometric characteristics or measures contained in a database are accessible only through an application contained in a system? How?

Have you planned to log all accesses to biometric data? Even for computer personnel?

Principle 6
Use of Biometric Data

The Act respecting information technology specifies that 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.

Do you ensure that the use of biometrics cannot serve to reveal characteristics about a person's health, mental condition and physical condition and any other information about a person? How?

Do you ensure that the information revealed by biometric data may not be used as a basis for a decision regarding the person concerned or for any other purpose? How?

Principle 7
Communication of Biometric Data

Biometric data remains confidential as long as the person concerned has not consented to its disclosure. Hence, the communication of biometric data requires the written consent of the person concerned.

In respect of information revealed by biometric data, the Act respecting information technology specifies that such information may only be disclosed to the person concerned, at the person's request.

What communications of biometric data are planned?

Do you ensure that all communications will be authorized by the written consent of the person concerned? How?

What will the form of consent be?

Do you ensure that the recipient meets the necessity requirements when biometric data are transmitted to him or her (with consent)? How?

Principle 8
Destruction of Biometric Data

The Act respecting information technology sets out that the biometric data and any notations 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. Accordingly, a person is obliged to destroy biometric data when these conditions are satisfied. The retention of this type of data for a longer period is therefore illegal.

What mechanisms do you use to determine whether the purpose of verification or confirmation of identity has been met or the reason for the verification or confirmation no longer exists?

Do you ensure that biometric data are destroyed immediately under these conditions? How?

What mechanisms do you use to irreversibly destroy all existing copies of biometric data?

Principle 9
Rights of Access and Correction

The right of access and correction by the person concerned set out in the Act respecting Access and the Act respecting the private sector is maintained in respect of personal information and biometric information. Biometric information held must therefore be able to be communicated intelligibly to any person wishing to exercise his or her a right of access and correction.

Can a person access his or her biometric data? How?

Can a person access data revealed by his or her biometric data? How?

Can the data be communicated to a person intelligibly? If so, through what mechanism?

Can a person exercise his or her right of correction? How?