



Commission
d'accès à l'information
du Québec

Pandemic, privacy and protection of personal information

Considerations regarding the use of certain technologies
(e.g. contact tracing, activity trackers, use of location data)



Document updated on 4 May 2020



BACKGROUND

Québec, like the rest of Canada and other countries throughout the world, is in the midst of an unprecedented health crisis. Difficult choices have been made, and have disrupted our lives. Government authorities, under the powers granted to them by the *Public Health Act* when a health emergency is declared, have introduced a set of measures designed to protect public health.

These measures have had a major impact not only on our daily lives, but also on public health and on Québec's economy. A gradual resumption of certain activities is now being planned, for when the timing is right. Technological initiatives continue to emerge or are under development throughout the world, with the aim of supporting the resumption of economic activity while helping to limit the pandemic. They include location data sharing, contact tracing applications, electronic alerts for breach of isolation orders, infection risk assessment applications and so on. Some countries are already using these types of devices and applications, while others are considering it.

As it has been pointed out, however, these tools are not without consequences for fundamental rights such as the right to privacy, the risk of discrimination, and so on. The issues they raise must therefore be considered carefully before such tools are implemented in Québec, because our values and legal framework are different from those of some of the countries that have introduced these solutions.

Despite the scope of the current crisis and the need for Québec to state its position on this matter quickly, a prior assessment and weighing of the values at stake is necessary to make an informed decision and well thought-out choices. The current "pause" in Québec suitable time for this process of reflection.

As part of its role of promoting the protection of personal information, the Commission d'accès à l'information would like to play a role in this process by proposing certain considerations in connection with the issues of privacy and protection of personal information that are likely to arise if these devices and applications are used. This document will not analyze the tools themselves, nor will decide whether or not they are appropriate or compliant with current legislation. It will, however, summarize the elements that must be considered before deciding whether or not to implement or use them in Québec, and where possible, will suggest additional guidelines to support the process of reflection.

This document may be updated as needed, to reflect the rapidly changing context.



PROTECTION OF PERSONAL INFORMATION AND PRIVACY

First, it may be useful to begin by reviewing the notions of privacy and protection of personal information.


Respect for private life is a fundamental right under Québec's *Charter of Human Rights and Freedoms* (s. 5). It was also protected in 1948, in the United Nations' *Universal Declaration of Human Rights* (art. 12). As a right, it is important not only at the individual level (e.g. autonomy, freedom, privacy, dignity, protection of a private sphere required for psychological well-being, the right to control the use of one's image) but also at the collective level in a democratic society (e.g. avoiding surveillance of individuals, protecting a person's domicile from abusive search and seizure). The right to respect for private life can also be tied to respect for other rights, such as protection from discrimination, the right to autonomy, freedom of circulation or opinion, and a person's right to safeguard his or her honour, dignity and reputation, etc.

However, the right to privacy, like every other fundamental right, is not absolute. Among other things, it must be exercised with proper regard for democratic values, public order and the general well-being of the citizens of Québec. The law therefore provides that it can be infringed in specific circumstances and on certain conditions, to ensure a balance and equilibrium between the needs of society and the rights of individuals. Among other things, infringement of a fundamental right may be justified if it can be shown that the measure in question aims to achieve a legitimate, serious and important objective and that the infringement is proportional to that objective. In such cases, the Charter provides that the law can then set the scope and limits to the exercise the right.

The **protection of personal information** is one dimension of the right to respect for private life: the information dimension. Québec has two Acts that protect personal information, one applicable to the public sector and the other to the private sector. They prevail over all Québec's other legislation, reflecting the importance of these rights within our society.

Their objective is to set out the rules that allow individuals to control their personal information, and to place limits on what public bodies and private enterprises can do in situations where they must collect and use information as part of their activities. Protecting personal information does not mean simply ensuring that it remains confidential. It also involves compliance with a set of rules designed to limit invasions of individual privacy through the collection, use, communication and storage of personal information. Two of the basic principles underlying these laws are to reduce the collection and use of personal information to a strict minimum, and to obtain consent from the person concerned.

Although the legislation certainly needs to be brought up to date, the principles on which it is based can still serve as a landmark for the considerations proposed in this document.



When considering the impacts of technological solutions, a two-step assessment is required. The first step balances the objective of the solution (is it necessary?) and its impact on individual privacy (is the invasion proportional to the objective?). If, and only if, the conclusion from this first step is that the objective justifies the solution and that the ensuing invasion of privacy is proportional to the objective, then the second step, namely to ensure that the terms and conditions of the solution are consistent with the principles and best practices associated with the protection of personal information, can be taken.

1 – Is the invasion of privacy justified and proportional?

Valid objective (is it necessary?)

The first consideration addresses the objective of the proposed technological solution. This objective is critical in assessing whether or not it is proportional to the proposed action


The objective should be sufficiently important to justify the limitation of a right protected by the Charter. It must be valid and relevant to a real, urgent social concern.

The objective of the technology itself must therefore be questioned. Obviously, the aim of all these technologies is to eradicate COVID-19 and limit the spread of the virus. However, it is important to clarify this by answering the following questions: How is the application or device likely to do this? What, specifically, does it aim to do with respect to the pandemic? For example, will it help public health authorities to carry out epidemiological surveys, trace contacts or obtain a more general profile of the disease's prevalence within the population? Or is its aim to ensure compliance with self-isolation measures by carriers of the virus? Or to identify people who may have been in contact with infected people, and if so, the reason why (tracing, recommendation of health measures, profiling, etc.)? Or to give advice to people based on their "level of risk", symptoms or potential contact with infected people? And so on.

A further question to ask is how consistent this objective is with the current public health strategy. Since the Government has declared a health emergency, the validity of any measure or solution that would hinder the actions of the public health authorities would be questionable, especially if it also infringed a fundamental right. In addition, there is the question of who proposed and developed the solution and established its objective. Was it a public body? The public health authorities? A private enterprise? Or another group? Are there any other, secondary objectives? If so, are they lawful?

Proportionality of the proposed measure

Furthermore, the designers of these solutions or the government authorities that adopt or promote them must demonstrate that the solutions are reasonable and can be justified, i.e. that the invasion of privacy they require is proportional to the objective or situation



being addressed. It is a matter of finding a balance between the means chosen to address the problem and respect for individual rights.

Proportionality is assessed using a three-step process.

1) First, there must be a **rational connection** between the pursued objective (including secondary objectives if any) and the proposed solution, i.e. the solution must provide an effective way of achieving the objective(s).

In practical terms, this means asking the following questions: Is it reasonable to conclude that the proposed solution will in fact achieve the objective? How, concretely, will the proposed application or technology achieve this objective? How will the collection, use or communication of personal information help to achieve this? How effective is the device (or at least, how effective is it expected to be, based on real, scientific data and a rational, objective assessment)? Has the device been effective in fighting COVID-19 elsewhere? If so, within what parameters? Was it combined with another measure, such as a testing or another policy?

2) Secondly, because privacy is a fundamental right, **any infringement of an individual's right to privacy must be minimal** and must only take place if **there is no other effective solution** that is less intrusive.


This involves questioning the scope of the proposed solution and asking whether other, less intrusive means would provide an effective solution or help achieve the objective. For example: Could the objective be achieved in another way, without invading individual privacy, without collecting or using personal information? What could be done to minimize any invasion of privacy? Should the use of this type of device or application be regulated specifically to the current context, because of the major privacy issues it raises? If so, how?

The nature of the information that would be collected and used will affect the assessment. The use of sensitive information, such as health-related information (e.g. a positive result to a Coronavirus diagnostic test, or symptoms) or information on a person's location, is more intrusive than the use of aggregate or other types of information.

Where the information is stored (centralized or decentralized) is also relevant to the assessment, as well as the circulation and accessibility to the information. For how long will the information be stored?

The secondary objectives or uses associated with the proposed solution must also be considered. Are they essential? Do they represent an additional invasion of privacy? If so, can these additional objectives or uses of personal information be removed?

What measures are provided to put a stop to the invasion of privacy at the end of the pandemic? Will the application be withdrawn from the market? Will the data be destroyed?



3) Last, the concrete **benefits** of the proposed solution **must outweigh the damaging consequences** for individuals.

This is basically a balance between the real benefits and disadvantages of applying the proposed technological solution. What are they? Do the benefits for the collective good outweigh the infringement of individual rights?

All the potential consequences likely to occur should be considered. For example, is the proposed measure likely to infringe other rights, such as the right to dignity or the right to safeguard one's reputation? Is it likely to cause discrimination or to stigmatize certain individuals? Might it have a positive or negative impact on measures adopted by the authorities to fight the pandemic (e.g. by creating a false sense of safety among the general public, or conversely, needlessly worrying people, contradicting public health directives, undermining public trust in the authorities, contradicting certain voluntary measures, etc.)? Is the solution consistent with the current testing strategy? Is it designed to facilitate epidemiological surveys? Will it add tasks or increase the current workload of medical staff, including public health officials, who are already overworked? Do the issues change, depending on whether the information is collected and used by the public authorities or by a private enterprise? If the application is available for use on a voluntary basis, what are the advantages and disadvantages of this approach?

If the conclusion from the first part of the assessment is that the proposed solution is justified and necessary in the current context, and that the ensuing invasion of privacy is proportional and allows for a balance between the needs of society and the rights of individuals, then the next step is to assess the conditions of application, to ensure that they are consistent with the principles and best practices for the protection of personal information in Québec.

2 – Compliance with principles and best practices for the protection of personal information

As mentioned earlier, protecting personal information does not simply mean maintaining the confidentiality and security of information concerning individuals. On the contrary, it involves the application of a set of principles and good practices designed to structure and minimize the collection, use, communication and storage of personal information.

It is important to refer to the appropriate legislation, depending on who will be collecting personal information through the proposed technological solution: a public body, a private enterprise or both. Public bodies must comply with the provisions of the *Act respecting Access to documents held by public bodies and the Protection of personal information*, and private companies must comply with the *Act respecting the protection of personal information in the private sector*.

The Commission would like to draw attention to the following non-exhaustive list of principles and good practices:



1. Prevention

Before implementing a technological device or application that involves the collection, use or communication of personal information, it is important to ensure compliance with the legislation and generally accepted principles governing the protection of personal information and privacy. This process, known as a Privacy Impact Assessment or PIA, is mandatory in many countries and in some Canadian provinces. It is used to identify issues from the early stages onwards, and ensures that solutions can be adjusted so that they are compliant and have minimal impacts for privacy.


A PIA examines all the factors that affect the protection of personal information and respect for privacy, either positively or negatively. The assessment involves an analysis that:

- > presents the project (objective, internal procedures, etc.);
- > identifies the personal information targeted by the project, and how it circulates within the information system (information life cycle);
- > describes the project's repercussions for the personal information;
- > links the project to the legal principles governing the protection of personal information (purpose of the file, necessity, collection, information, use, consent, communication, destruction, safety, access, etc.);
- > identifies risks and consequences for the protection of personal information;
- > identifies and implements ways to minimize invasions of privacy and to protect personal information.

A PIA is an iterative process that monitors the development of the application and is revisited each time changes or additions are made.

For additional details: https://www.cai.gouv.qc.ca/documents/CAI_FI_efvp.pdf (in French only). A preliminary guide (in French only) will shortly be available on the Commission's website: <https://www.cai.gouv.qc.ca/>.

Another good preventive practice is to design intended solutions or applications by integrating the privacy and personal information protection principles from the beginning (privacy by design) or by default (privacy by default). Privacy by design, as its name suggests, consists in designing a solution that maximizes respect for privacy at every stage of development, from needs analysis to design, during implementation, and during audits and maintenance, including decommissioning, whether voluntarily by the user or at the end of the solution's useful life. These measures must be applied to every stage of the information life cycle (from collection to destruction) and be transparent (users must be told about them). As for privacy by default, it involves ensuring that all the application's default settings provide maximum data protection (i.e. without the user having to choose the settings that offer the highest level of protection).



Some technological developments may also be used to improve the protection of personal information. These are known as privacy enhancing technologies or PETs. For example, they can help limit the collection of personal information (e.g. data anonymization), enhance confidentiality or security, limit access to certain people or improve a person's control over his or her own personal information (e.g. pseudonymization, differential privacy, cryptography, homomorphic encryption, cryptographic hashing, selective disclosure techniques, data tagging, etc.). For examples of these different techniques, see: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/.

2. Limit collection to necessary personal information only


One of the most important legislative principles for the protection of personal information is that collection must be limited solely to personal information that is necessary. This rule cannot be circumvented by consent: in other words, a private enterprise or public body cannot collect unnecessary personal information even if the person concerned has given consent.

It must therefore be possible to explain and prove necessity when collecting personal information. This involves considering how each piece of information will help to achieve the proposed solution's objective. Here too, proportionality is important in determining necessity. In other words, the nature of the information to be collected must be established, and every possible measure must be taken to minimize the impact on the person's privacy.

For example, if the information in question is sensitive, the measures taken to minimize the invasion of privacy must be more significant, and all other means of achieving the objective must be used first. However, if the objective can be achieved by collecting anonymized, depersonalized, pseudonymous or aggregate data, then this is the path that must be taken. If less sensitive information is available, it should be collected instead, or reasons should be given to show why it is less effective. For example, some contact-tracing applications use geolocation data, while others use proximity information (Bluetooth) only, which does not involve surveillance or monitoring of movement.

The following clarifications will help you determine the nature of information that is collected.

- > **Personal information:** Information is personal if it concerns and can be used to identify a natural person. The assessment of the criterion "Can be used to identify" refers to the ability to distinguish the person from someone else and to maintain a connection between the person and the information concerning him or her.
- > **Sensitive personal information:** The "sensitive" nature of information is determined by its intimate nature or by the harmful consequences that would arise from its disclosure. For example, health-related, taxation, financial or genetic



information, or information concerning a person's sexuality, would be classified as "sensitive", as would information associated with the risk of discrimination (race, ethnic origin, religion, handicap) or identity theft (contact information, unique identifiers such as a person's health insurance number, driver's licence or social insurance number). Biometric data, which is unique, permanent and intimate, also falls into this category. See section 6.1 of this document for additional information on the nature of biometric data and the specific rules applicable to it.


- > **Anonymous information:** Information is anonymous if it cannot be used to identify an individual and if anonymization is irreversible even with the use of other information or re-identification techniques. The removal of direct identifiers (name, address, health insurance number, driver's licence number, IP address, etc.) is insufficient to anonymize information. Anonymization must be irreversible. Before concluding that information has been anonymized, the risk of re-identification must be carefully analyzed and proved.

It can be challenging to anonymize certain data because of their nature. For example, it may be fairly easy to deduce a person's home or work address, and hence his or her identity, from geolocation data.

- > **Depersonalized information:** This is personal information from which direct identifiers have been removed, or from which it is impossible to identify an individual without using other information, a match key or re-identification techniques. There are a number of depersonalization techniques, including pseudonymization (replacing direct identifiers by digital or other pseudonyms), encryption, and so on. However, it is important to remember that this type of information is still personal information and is therefore subject to all the legislative rules governing the protection of personal information.
- > **Inferred personal information:** Some projects may require the use of artificial intelligence systems whose algorithms can infer new information from collected information: for example, your risk level of being infected by the virus or of having been in contact with an infected person. When this inferred information concerns and can be used to identify a natural person, it becomes personal information and is subject to the legislative rules governing personal information. This means that a private enterprise or public body holding inferred information must comply with the requirements for the protection of personal information, including the need to limit its use and communication as required by law, ensure that it remains confidential, and destroy it. The individual concerned is also entitled to access the information and rectify it where necessary.

3. Transparency

The legislation governing the protection of personal information provides that individuals must be informed of certain elements when personal information is collected. The same



applies when consent must be obtained in order to use or communicate personal information to a third party. Lastly, public bodies and private enterprises must show that they are acting responsibly by being transparent about the steps they have taken to protect personal information.


Before the application is used, transparency can be shown by indicating, in complete, simple, easy-to-understand terms:

- which information is being collected: list all the information, including any that will be inferred by an algorithm. Special attention should be paid to the descriptors used; as noted earlier, depersonalized information is not anonymized.
- the purposes for which the information will be used: describe all the proposed uses and specify which information will be used in each case.
- if the information will be processed automatically, via an algorithm, explain the most important factors and parameters that will be used for decision-making, prediction or profiling. What is the underlying logic of the processing mechanism? Which personal information will be used in this way?
- who will have access to which information: be precise and state why it is necessary for these categories of people or these other bodies or enterprises to have access to the information.
- where the information will be stored.
- what have been the measures taken to ensure that the information remains confidential and secure throughout its life cycle.
- how individuals can exercise their right of access to and rectification of information that concerns them: appoint someone to be responsible for this and provide contact details. The person can also answer questions and address concerns raised by individuals regarding the way your organization protects their personal information.

4. Limit the use and disclosure of personal information

The legislation applicable to the public and private sectors provides that information collected can be used only for the purposes for which it was collected, or for purposes that are consistent with them. Given the sensitive nature of the information required by many of the applications currently in use or described by the media as being under development, combined with the high level of intrusiveness and the likelihood that these applications will infringe other fundamental rights, the use of personal information should be limited to the purposes stated during the collection process.

Similarly, personal information should also be depersonalized or anonymized wherever possible.



The legislation also provides that information cannot be communicated to third parties without the consent of the person concerned or without legal authorization. Additional requirements apply to the communication of personal information outside Québec, including the obligation to ensure that the information will be given a level of protection equivalent to that required by law in Québec.

5. Consent

Some of the principles arising from our democratic values and our fundamental rights and freedoms serve as clear arguments to suggest that technology applications should be used only on a voluntary basis as solutions to the current situation. For other projects, including those that require the communication of personal information, consent is usually required, unless the law states otherwise.

To be valid, consent must be:

- > **Free:** expressed without conditions, constraints, threats or promises. A person may therefore withdraw his or her consent at any time.
- > **Informed:** given with awareness as to its scope, with full knowledge of the facts, hence the importance of transparency.
- > **Specific:** authorizing the use or communication of specific personal information, to specific people, for specific purposes and at a specific time. If there are plans to use or communicate the information for several different purposes, separate consent must be obtained in each case.
- > **Limited in time:** valid for the time needed to achieve the objectives for which the consent was requested.
- > **Manifest:** expressed clearly and unequivocally. If it relates to sensitive information, it must be express, i.e. given in writing.

For some of the applications described in the media, effectiveness appears to depend on the extent to which the public adopts them, and it has been a suggestion that incentives, or even social pressure, would be desirable. However, this would cast doubt on the free and informed aspects of consent and would impact the measure's proportionality to the ensuing infringement of rights.

The possibility that an application may become a *de facto* condition for entry into a building, store or workplace must also be considered. This includes the risk that a person using an application may be forced to disclose personal information: level of infection risk, declared symptoms, results of virus testing, recommendations by the application, etc. Not only does this cast doubt on consent, but the risk of service denials and infringements of other rights must also be considered when deciding whether or not to use these applications.



6. Assess the impacts of using artificial intelligence systems

If the use of an artificial intelligence system (or automated information system) involving personal information is being considered, the Commission feels that a number of principles should be implemented, even though they are not currently part of Québec's personal information legislation, which is outdated in this respect.

Some of these principles have been covered by preceding sections of this document. Others, however, including those relating to governance and liability, must also be considered. For example, it may be appropriate to assess the algorithmic impacts of an automated system. For an example of this, see: <https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai/algorithmic-impact-assessment.html>

For further details regarding the principles and features of the protection of personal information as they apply to the use of artificial intelligence, the Commission's consultation document (in French only) can be found [here](#).

Although these documents have not yet been finalized, they may nevertheless be useful in the current exceptional circumstances.

6.1 Comply with the specific rules applicable to biometric information and geolocation data

Geolocation


Section 43 of the *Act to establish a legal framework for information technology* (CQLR, c. C-1.1; hereinafter the ALFIT) limits the use of a device that allows the person's whereabouts to be known, such as a device that provides geolocation data: [...] "*Unless otherwise expressly provided by law for health protection or public security reasons, a person may not be required to be connected to a device that allows the person's whereabouts to be known.*"

Biometric data

A public body, private enterprise or any other organization considering the use of biometric measures or characteristics to achieve the objective of preventing COVID-19 must take the specific nature of biometric data into account.

The term "biometrics" refers to a technique that uses one or more pre-recorded unique physical or behavioural characteristics to verify the identity of a person who wishes to perform an action.

There are two main categories of biometrics:

- 
- > **Morphological biometrics**, which identifies specific physical traits. This category includes fingerprint, hand shape, retina and iris recognition.
 - > **Behavioural biometrics**, which analyses aspects of a person's behaviour such as handwritten signature, voice print, gait, keyboard strokes and so on.

This information, whether in raw (image or print) or digital (algorithm-derived code) format, constitutes sensitive personal information to which additional rules apply. These rules are set out in sections 43 to 45 of the *ALFIT*.

The Commission has published documents that provide information for biometrics-based initiatives. They include an information sheet entitled [La biométrie au Québec](#) (available in French only) and a document entitled [Biometrics in Québec: Application Principles – Making an Informed Choice](#). Other information tools are currently under preparation.

7. Destroy personal information

Personal information must be destroyed when the purposes for which it was collected have been accomplished. Health-related and geolocation data are highly sensitive, and these are the types of data generally required for the projects described in the media or applied in other countries. It is vital that they be destroyed because of the infringement of fundamental rights and freedoms that they represent.

8. Allow the person concerned to exercise their rights

The law provides that individuals have the right to access and rectify personal information that concerns them. How can individuals exercise this right with respect to the information collected by some of the proposed solutions, and with respect to information inferred by algorithms?

9. Structuring, reporting, independent external controls and reassessment

Any solution that involves collecting, using or communicating personal information should also be subject to governance measures and be supervised by an independent control authority.

The organizations responsible for these devices and applications should issue regular public reports on the effectiveness of:

- > the measure itself, in achieving the health-related objective, and the relevance of maintaining it;
- > the measures introduced to protect personal information and minimize invasions of privacy.



CONCLUSION

This document does not attempt to list all the issues and elements to be weighed when considering the relevance, legality and effectiveness of technology-based tools and devices; it simply sets out the elements that the Commission wishes to submit for consideration. The Commission reaffirms the importance of engaging in this process of reflection before deciding to proceed with the use of these tools, which should not be considered or implemented without a guarantee that individual privacy of citizens will be upheld and that every possible step has been taken to comply with the current legislation in Québec.

To continue the thinking process...

The following resources, while by no means exhaustive, may contribute to the present considerations provide additional food for thought:

- Commission de l'éthique en science et en technologie :
 - ✓ [Framework for reflection on the ethical issues of the COVID-19 pandemic](#) (in French)
 - ✓ Use of mobile artificial intelligence applications for COVID-19 surveillance in Québec:
 - [General information](#) (in French)
 - [Special committee interim report](#) (in French)
- [Traçage des données mobiles dans la lutte contre le Covid-19 : Analyse des potentiels et des limites](#), by Mounir Mahjoubi (in French). See also this [summary](#) (also in French).
- [European Commission Recommendation on a common union toolbox for the use of mobile technology and data](#)
- [Letter of April 14, 2020 from the European Data Protection Board concerning a draft guide to the use of apps during the COVID-19 pandemic](#)
- [CDPDJ website](#) (content available in French only)
- [Letter from Dutch scientists and specialists from different fields](#)
- [Analysis of the risks of anonymous tracing for non-specialists \(version of April 21, 2020\)](#) (in French only)