A Framework for the Government of Newfoundland and Labrador to Assess Privacy-Impactful Initiatives in Response to COVID-19

Context

The Office of the Information and Privacy Commissioner (OIPC) in Newfoundland and Labrador is responsible for upholding and protecting access to information and protection of privacy rights in the Province of Newfoundland and Labrador. The jurisdiction of the OIPC extends to public bodies subject to the *Access to Information and Protection of Privacy Act* (*ATIPPA, 2015*), as well as custodians of personal health information subject to the *Personal Health Information Act* (*PHIA*).

The safety and security of the public is of grave concern in the current COVID-19 health crisis. The urgency of limiting the spread of the virus is understandably a significant challenge for government and public health authorities, who are looking for ways to leverage personal information and "Big Data" to contain and gain insights about the novel virus and the global threat it presents. In this context, we may see more extraordinary measures being contemplated. Some of these new measures may not be voluntary, and perhaps certain measures that are currently voluntary will become mandatory. Some of these measures will have significant implications for privacy and civil liberties.

During a public health crisis, privacy laws and other protections still apply, but they are not a barrier to the appropriate collection, use and sharing of information. When reasonably and contextually interpreted, existing privacy legislation, norms and best practices for data collection, use and disclosure ensure responsible data use and sharing that supports public health. They also promote continued trust in our health system and in government generally.

All public bodies and custodians must continue to operate under lawful authority and act responsibly, particularly with respect to handling personal health information, and information about individuals' travel, movements and contacts or association all of which are generally considered sensitive.

Privacy protection isn't just a set of technical rules and regulations, but rather represents a continuing imperative to preserve fundamental human rights and democratic values, even in exceptional circumstances. Public bodies and custodians should still apply the principles of necessity and proportionality, whether in applying existing measures or in deciding on new actions to address the current crisis. Purpose limitation, that is, ensuring that personal information collected, used or disclosed for public health reasons is not used for other reasons, is particularly important in current circumstances. How personal information is safeguarded, and how long it is retained after the crisis, is also crucial.

Office of the Information and Privacy Commissioner
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or 1-877-729-6309 Fax: (709) 729-6500
E-mail: commissioner@oipc.nl.ca www.oipc.nl.ca

The COVID-19 public health crisis has raised exceptionally difficult challenges to both privacy and public health. The following are key privacy principles that should factor into any assessment of measures proposed to combat COVID-19 that have an impact on the privacy of residents of the Province of Newfoundland and Labrador.

For further information regarding private industry and federal government departments which are outside the jurisdiction of the OIPC, the Office of the Privacy Commissioner of Canada (OPC) has issued guidance to help organizations subject to federal privacy laws understand their privacy-related obligations during the COVID-19 outbreak. For guidance on other privacy principles that continue to apply, please read Expectations: OPC's Guide to the Privacy Impact Assessment Process.

This Guidance is based on a similar piece published by the Office of the Privacy Commissioner of Canada, whose permission to adapt this for the Province of Newfoundland and Labrador context is gratefully acknowledged.

Framework

1) Legal Authority

Identify the legal authority to collect, use, and disclose personal information.

Key Messages

- All public bodies and custodians must continue to operate with lawful authority. This means, for public bodies, such as government departments, agencies, boards, and commissions, the *Access to Information and Protection of Personal Privacy Act, 2015 (ATIPPA, 2015)* govern their activities. For custodians of personal health information, the *Personal Health Information Act (PHIA)* applies.
- At the federal level, private-sector organizations that collect, use, or disclose personal information in the course of a commercial activity are subject to the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). The federal *Privacy Act* covers personal information-handling policies and practices of federal government departments and agencies. *PIPEDA* and the *Privacy Act* are under the jurisdiction of the federal Office of the Privacy Commissioner of Canada (OPC).
- Privacy laws apply to personal information, which is information about an identifiable individual. This is so even when public bodies or custodians use "open" or public sources such as social media. Some laws also allow for use of publicly available data under specific conditions. (See also principle four: de-identification.)

2) Necessity and Proportionality

Ensure the measures that public bodies and custodians take are necessary and proportionate.

The OIPC recognizes that the COVID-19 crisis is a rapidly evolving situation that requires swift and effective responses to address extraordinary public health needs. The right to privacy is not absolute. However, even in these challenging circumstances, government institutions should still ensure that their measures are necessary and proportionate, which means essentially evidence-based, necessary for the specific purpose identified and not overbroad.

Key Messages

- The public health purpose underlying a potentially privacy infringing measure must be science-based and defined with some specificity. It is not enough to simply state that a measure supports public health without being more precise.
- The measure must be tailored in a way that is rationally connected to the specific purpose to be achieved. If the purpose of a measure is to reduce the occurrence of large gatherings in public places, mass collection of all movements of a population would not be proportionate.
- The measure must be necessary; that is, more than potentially useful. Again, it must be evidence-based and likely to be effective. However, demonstrating effectiveness must be assessed in context. Also, necessity does not mean "absolute necessity" (i.e., that no other conceivable means are available, regardless of costs).

The OIPC has developed a guidance slide deck "Don't Blame Privacy – What to Do and How to Communicate in an Emergency" to inform public bodies and custodians about information collection, use, and disclosure during COVID-19 and other emergency situations.

The OIPC document Privacy Impact Assessments contains key questions for public bodies to consider that can assist public bodies and custodians in assessing the privacy impact of measures to address COVID-19.

3) Purpose Limitation

Personal information and personal health information collected, used or disclosed to alleviate the public health effects of COVID-19 must not be used for other reasons.

Key Messages

- This is particularly important in the current context, where more personal information or personal health information may be collected, used and disclosed than in normal circumstances. Individuals' reasonable expectation of privacy may be less in a public health crisis, but they would not reasonably expect that sensitive information (such as health or places or persons visited) would be available for other government or commercial purposes.
- Public bodies and custodians should continue to adhere to the minimum amount necessary standard when handling personal information and personal health information. (For more information on this topic, please review the OIPC guidance document on "Minimum Amount Necessary Requirement".
- Personal information collected in an emergency situation should also be destroyed when the crisis ends, except for narrow purposes such as ensuring accountability for decisions made during the crisis, particularly decisions about individuals. If a public body or custodian wishes to retain information for future evaluation or research, de-identification measures should be implemented. (See also principle nine: Time Limitation)

4) De-Identification and Other Safeguarding Measures

Use de-identified or aggregate data whenever possible.

Key Messages

- Consider whether identifiable information is required in the context, or if de-identified or aggregate data is sufficient.
- Be aware that there is always a real risk of re-identification, although it is generally less for aggregate data. It is important to be attentive to the risks, which are highly case-specific - dependent on what data is used, in what form, and with what other data it is combined, and with whom it will be shared.
- Be especially mindful about the unique challenges with location data:
    - Location data points themselves can lead to re-identification as they can reveal personal details, such as the location of an individual's home, routine behaviours, and associations.
    - Precise location data, particularly in real-time, can be very challenging to fully anonymize or de-identify.
- Take administrative, technical and physical means to protect the personal information collected. Ensure safeguards are enhanced for sensitive information.

5) Vulnerable Populations

Consider the unique impacts on vulnerable groups.

Key Messages

- Consider how certain information, such as health and precise location data, may have greater sensitivities or disproportionate impacts on vulnerable populations and certain groups of individuals, for example:
  i. For some individuals, the collection of health-related data concerning gender, gender identity and expression is of even greater sensitivity.
  ii. Data sets on populations, or subsets of populations, may affect different subgroups or communities with disproportionate consequences.
  iii. Algorithmic decision-making or AI may contain inherent biases that could create disproportionate impacts.

6) Openness and Transparency

Provide clear and detailed information to residents about new and emerging measures, on an ongoing basis.

Key Messages

- Transparency is a cornerstone of democratic governance, as well as our privacy laws. It is all the more vital in the midst of a crisis, when extraordinary measures are being contemplated.
- The public, and wherever possible individuals, must be informed of the purpose of the collection of their personal information.

7) Open Data

Carefully weigh the benefits and risks of the release of public datasets, giving particular attention to health and location data, and impacts on vulnerable populations.

Key Messages

- An assessment of how granular public datasets should be is context-specific.
- Even with the release of aggregate data, be attentive to the impacts on vulnerable populations, subsets of populations, and groups. Give particular attention when geolocation data is involved, as it can disproportionately impact marginalized and vulnerable communities.

8) Oversight and Accountability

New laws and measures specific to the crisis should also provide specific provisions for oversight and accountability.

Key Messages

- Institutional safeguards become more, not less, important during times of crisis.
- New laws should contain provisions for oversight and accountability.
- Subject to section 112 of the *ATIPPA, 2015*, any Bill which may impact access to information or protection of privacy rights shall be subject to consultation with the Commissioner as soon as possible before, and not later than the date notice is given to introduce the Bill in the legislature. The Commissioner should be engaged as early as possible in the process so as to allow for sufficient opportunity for the Commissioner to review and comment on the Bill without impeding the timeliness of important legislative initiatives.

9) Time Limitation

Privacy invasive measures should be time-limited, with obligations to end when they are no longer required.

Key Messages

- There should be strict time and other limits on measures implemented in response to the crisis (e.g. type and range of personal data collection, sharing, and use). Time limits should be conservative, with the option to extend.
- Personal information and personal health information collected in an emergency situation should also be destroyed when the crisis ends, except for narrow purposes such as ensuring accountability for decisions made during the crisis, while de-identifying information retained for research purposes.