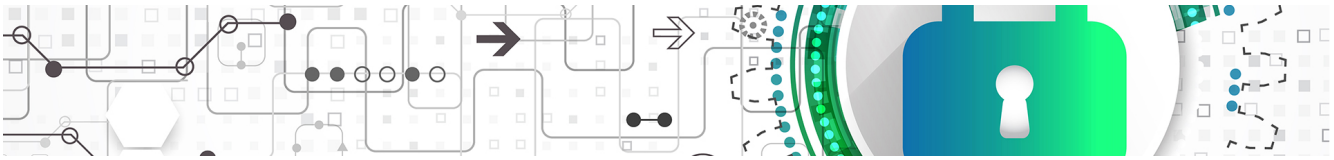

COVID-19 and Privacy: Federal Privacy Commissioner Publishes Framework to Help Government Institutions Assess Privacy-Impactful Initiatives

April 27, 2020

By Amanda Branch

On April 17, 2020, the Office of the Privacy Commissioner of Canada (the "OPC") published an assessment framework, "A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19". This framework is intended assist government institutions and help "guide the development of privacy impactful initiatives that seek to alleviate the effects of the pandemic".

The OPC recognizes the current public health crisis calls for a "flexible and contextual application of privacy laws"; however, organizations must continue to operate under lawful authority, and the principles of necessity, purpose limitation and proportionality continue to apply. The framework sets out the following key privacy principles. While this particular framework is targeted at government institutions, it includes some references to private-sector organizations and how these principles are equally applicable.

1. **Legal Authority**. Organizations must have a clear legal basis for the collection, use and disclosure of personal information. Privacy laws apply to "personal information" which is generally defined as information about an identifiable individual. This may include information found on "public" sources like social media.
2. **Necessity and Proportionality**. While the COVID-19 pandemic is a rapidly evolving situation, government institutions must ensure the proposed measures are necessary and proportionate which, in this instance, means evidence- or science-based and necessary for a specific identified purpose.
3. **Purpose Limitation**. Personal information should be used only for the purpose for which it was collected. In this context, that means personal information collected for the purpose of protecting public health should not be used or disclosed for any other government or commercial purpose.
4. **De-identification and other safeguarding measures**. The framework encourages the use of de-identified or aggregated data whenever possible. Generally speaking, information that is truly de-identified is not considered personal information and is therefore not subject to privacy legislation. We have written about the use of de-identified information, including the importance of minimizing the risk of re-identification. The framework also notes unique challenges associated with location data, specifically that location data points can lead to the re-identification of an individual and, in particular, the location of his/her home or routine behaviours.
5. **Vulnerable Populations**. Consider how certain information may have disproportionate impacts on vulnerable populations. For organizations making use of AI, steps should be taken to help reduce the introduction of bias.
6. **Openness and Transparency**. Transparency is a cornerstone of privacy legislation. Individuals must be informed of the purpose of the collection of their personal information. The framework also states that clear and detailed information about new and emerging measures should be provided to Canadians on an on-going basis.
7. **Open Data**. We have written about the importance of making data publicly available, within reason and by making use of de-identified data. The framework states that before releasing public datasets the benefits and risks should be carefully assessed. This assessment should be context specific and should consider any particular risks (e.g., location data) or disproportionate impact on subsets of populations.
8. **Oversight and Accountability**. An organization is responsible for the personal information under its control. Institutional safeguards continue to be important during times of a crisis and any new measures specific to the crisis

should also provide specific provisions for organizational oversight and accountability.

9. **Time Limitation**. Personal information should not be retained indefinitely. This includes personal information collected in an emergency situation which should be destroyed when the crisis ends (except in narrow circumstances). Further, any privacy invasive measures should be time-limited and should cease when no longer required.

This framework compliments the previously issued guidance on applicable federal privacy laws and the collection, use and disclosure of personal information in the context of a public health crisis. Numerous provincial and territorial privacy regulators have also released similar guidance documents for organizations subject to legislation in their respective jurisdictions. The framework invites organizations (governmental or private-sector) to reach out to the OPC with questions.