THE ROAD TO A "NEW NORMAL": CONTACT TRACING AND PRIVACY CONSIDERATIONS IN CANADA

Posted on June 1, 2020

Categories: Insights, Publications

Provinces across Canada are starting to lift COVID-19 restrictions and resume some economic and other activities. As we pave our way into a “new normal”, governments are considering the implementation of certain measures to avoid a surge of new infections. Countries at more advanced stages of reopening their economies such as Taiwan, South Korea and Singapore have adopted contact tracing mobile applications as one of the measures to contain the virus until a vaccine is available.

This bulletin reviews privacy concerns relating to the public implementation of contact tracing apps and guidance from Federal and Provincial Privacy Commissioners on how such concerns may be resolved.

Contact tracing, explained

Contact tracing is a process of identifying individuals who may have come into contact with, or have been in close proximity to, an infected person. Contact tracing apps have the ability to identify and notify individuals who have had recent contact with an infected person an anonymized basis. It is possible to operate contact tracing apps on either a centralized or a decentralized basis. The centralized apps work by uploading the anonymized data to a central system, which is typically controlled by a government institution. The decentralized apps keep the data on the user’s phone, which gives the user more control over the data.

Many consider contact tracing an essential tool for public health officials and local communities to fight the spread of COVID-19 and has been identified as a key element for reopening economies across different provinces in Canada. The Province of Ontario’s guidelines for reopening its economy published in April 2020 stipulate that one of the key principles that will guide this process is the capacity to trace and isolate the virus. As of the date of this writing, however, Alberta is the only Province that has implemented a contact tracing app.

Resolving privacy concerns with contact tracing

Contact tracing apps raise privacy concerns because they involve collection, use, and disclosure of sensitive personal data, including health information and geo-location data points.

The Office of the Privacy Commissioner of Canada (the "OPC") published an assessment framework to guide government institutions implementing privacy impactful measures – such as contact tracing apps – to respond to the COVID-19 pandemic. The assessment framework sets out key guiding privacy principles that government institutions should consider when adopting potentially intrusive measures without decreasing usefulness to public health.

The following have been identified as the key privacy principles for government institutions implementing contact tracing apps to consider:

1. Legal authority

There must be a clear legal basis to collect, use, and disclose personal information and any consent obtained for the collection must be meaningful. In this regard, consent must be obtained for all specific public health purposes.

2. Contact tracing must be necessary and proportionate

The OPC is aware that the pandemic requires government institutions to take extraordinary measures. However, in doing so, it is important to protect Canadians' right to privacy. Government institutions adopting contact tracing apps as a measure to contain COVID-19 have to ensure that this is implemented in a proportionate and minimally intrusive manner and that there is scientific backing for the measures being undertaken.

3. Purpose of contact tracing must be limited to strictly protecting public health

Contact tracing apps should not collect, use and disclose sensitive personal information other than for the intended specific public health purpose.

4. Contact tracing measures should use de-identified or aggregate data whenever possible

Personal information should be de-identified, if possible. Because contact tracing apps have the ability to collect, use and disclose location data points including precise location data in real-time, there is a high risk of re-identification. The risk of re-identification should be considered and mitigated to the extent possible.

5. Vulnerable populations

The collection, use and disclosure of sensitive personal information such as health information and location data may have a detrimental impact on vulnerable populations. It is imperative that vulnerable populations are identified and measures are built into contact tracing apps to protect these populations without compromising their ability to benefit from the apps during the crisis.

6. Openness and Transparency

Openness and transparency are the cornerstone of Canadian privacy laws. These principles are emphasized when extraordinary measures are being considered to address the COVID-19 crisis. Government institutions adopting contact tracing apps should ensure that they provide the public with detailed information about these apps on an ongoing basis.

7. Time Limitation

Personal information collected by contact tracing apps should be destroyed when it is no longer required for the intended public health purposes.

A joint statement by Canada's the Federal, Provincial and Territorial Privacy Commissioners urges governments seeking to implement contact tracing through mobile apps to respect the following privacy principles in addition to those mentioned above:

1. Consent and Trust

The use of contact tracing apps must be voluntary and governments must demonstrate transparency and accountability in order to preserve public trust and confidence.

2. Safeguards

Governments must use appropriate legal and technical safeguards to protect the information collected using contact tracing apps. Safeguards must include contractual measures with developers and service providers to preclude unauthorized access and that data is used only for its intended public health purpose.

Key Takeaways

As governments begin to reopen economies across Canada, it is anticipated that they will install safeguards to help reduce the risk of subsequent waves of infection. Certain safeguards, such as contact tracing, have the potential to impede on the privacy rights of Canadians. While securing public health and safety is paramount, Privacy Commissioners across the country urge that governments have regard to key privacy principles when doing so.

Government institutions, companies and organizations who are involved in the design, implementation or support of contact tracing apps should consider the key privacy principles outlined above and all other applicable obligations pursuant to Canadian privacy laws. McMillan's team of privacy lawyers are available to respond to questions and provide advice as Canada's Federal and Provincial governments set the foundation for the "new normal".

by Chiedza Museredza, Mitch Koczerginski

a cautionary note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.