Office of the Information & Privacy Commissioner
OIPC
Nova Scotia

Supporting public health, building public trust:
Privacy principles for contact tracing and similar apps

Joint Statement by Federal, Provincial and Territorial Privacy Commissioners[1]
May 7, 2020

The safety and security of Canadians is of grave concern in the current COVID-19 health crisis. The urgency of limiting the spread of the virus is a significant challenge for government and public health authorities, who are looking for ways to leverage personal information[i] 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 measures will have significant implications for privacy and other fundamental rights. The choices that our governments make today about how to achieve both public health protection and respect for our fundamental Canadian values, including the right to privacy, will shape the future of our country.

One of the measures currently being contemplated or already being implemented in some jurisdictions within Canada and around the world is the launch of smart phone apps as a public health tool. Many of these apps are either for the purposes of contact tracing or for purposes of notifying individuals of the fact that they have been in close proximity of someone who has been confirmed or is assessed as likely to be a carrier of COVID-19, in order to help prevent further spread of the virus.

Commissioners felt it important to issue a common statement to Canadians because these applications raise important privacy risks. While applicable privacy laws must be observed, some of them do not provide an effective level of protection suited to the digital environment, as was highlighted in a joint resolution last fall. This is why we invite our respective governments, insofar as they plan to use contact-tracing applications, to respect at least the following principles:

- **Consent and trust:** The use of apps must be voluntary. This will be indispensable to building public trust. Trust will also require that governments demonstrate a high level of transparency and accountability.

- **Legal authority:** The proposed measures must have a clear legal basis and consent must be meaningful. Separate consent must be provided for all specific public health purposes intended. Personal information should not be accessible or compellable by service providers or other organizations.

[1] The Information and Privacy Commissioner of Alberta is reviewing a privacy impact assessment for the ABTraceTogether app that was recently launched in Alberta, and will provide recommendations directly to the Government of Alberta.

- **Necessity and Proportionality:** Measures must be necessary and proportionate and, therefore, be science-based, necessary for a specific purpose, tailored to that purpose and likely to be effective. To assist in determining whether the measure in question is justifiable in the circumstances, governments should consider the following:

    - **Necessity:** the public health purpose or purposes underlying a measure must be evidence-based and defined with some specificity. Is the purpose to notify users and advise them to take certain actions? Is it to assist public health authorities to better understand local conditions for resource allocation purposes? Is it for another purpose?
    - **Proportionality:** the measure should be carefully tailored in a way that is rationally connected to the specific purpose(s) to be achieved,
    - **Effectiveness:** the measure must be likely to be effective at achieving the defined purpose(s), and,
    - **Minimal intrusiveness:** while the least intrusive option for the intended purpose should be chosen, and data minimization should be applied, where that cannot be achieved or demonstrated, governments should clearly communicate the rationale for the level of personal information that they need to collect.
- **Purpose Limitation:** Personal information must be used for its intended public health purpose, and for no other purpose.

- **De-identification:** De-identified or aggregate data should be used whenever possible, unless it will not achieve the defined purpose. Consideration should be given to the risk of re-identification, which can be heightened in the case of location data.

- **Time-Limitation:** Exceptional measures should be time-limited: any personal information collected during this period should be destroyed when the crisis ends, and the application decommissioned.

- **Transparency:** Government should be clear about the basis and the terms applicable to exceptional measures. Canadians should be fully informed about the information to be collected, how it will be used, who will have access to it, where it will be stored, how it will be securely retained and when it will be destroyed. Privacy Impact Assessments (PIAs) or meaningful privacy analysis should be completed, reviewed by Privacy Commissioners, and a plain-language summary published proactively.

- **Accountability:** Governments should develop and make public an ongoing monitoring and evaluation plan concerning the effectiveness of these initiatives and commit to publicly posting the evaluation report within a specific timeline. Oversight by an independent third-party – such as review and implementation monitoring by a privacy commissioner's office – will help ensure accountability and reinforce public trust. While some privacy commissioners have the legal authority to conduct independent audits, it is encouraged that others be given this mandate by government through appropriate means. If effectiveness of the application cannot be demonstrated, it should be decommissioned and any personal information collected should be destroyed.

- **Safeguards:** Appropriate legal and technical security safeguards, including strong contractual measures with developers, must be put in place to ensure that any non-authorized parties do not access data and not to be used for any purpose other than its intended public health purpose. Authorities must ensure the public are aware of associated risks and threats (e.g. online fraud or malware).