Cassels

Canada's Privacy Commissioners Outline Guidance for Governments and Developers of Contact Tracing Technology

May 13, 2020

Overview

The federal, provincial and territorial privacy commissioners released a joint statement on May 7, 2020, to address privacy principles implicated in contact tracing technology[1] (the Joint Statement). The Joint Statement recognizes that "extraordinary measures" may be taken to both trace and notify the public in an effort to limit the spread of COVID-19, including the development and implementation of smart phone apps or similar technologies that process personal information with "significant implications for privacy and other fundamental rights."

The federal government and several provincial governments including Ontario[2], have stated they will not rule out the potential use of personal information to trace COVID-19.[3] Ontario's Information and Privacy Commissioner confirmed that his office would not challenge such a development given the current circumstances, if the province's decisions were "correlative to the outbreak."[4]

General Principles

The Joint Statement outlines several principles to guide governments in developing and implementing "extraordinary measures" to trace and contain the spread of COVID-19. Technology companies are well advised to keep these principles in mind when developing applications or other information tracing technologies for public sector institutions, where personal information is collected:

- the institution must ensure that it has the legal authority to collect, use and disclose information as part of its proposed program, activity or initiative;
- measures must be necessary to an evidence-based public health purpose;
- use must be voluntary;
- meaningful consent must be obtained from users for each specific public health purpose;
- personal information must not be accessible or compellable by service providers or other organizations;
- measures must be proportionate to the specific purpose the measure is established to achieve, and for no other purpose;
- measures must be likely to be effective to achieve the specific purpose;

- measures chosen by governments must be the least intrusive option for the intended purpose;
- data minimization should be applied, and de-identified or aggregated whenever possible;
- measures should be time-limited, personal information collected must be destroyed, and the application decommissioned when the COVID-19 crisis ends; and
- safeguards must include contractual measures between governments and app developers to prevent unauthorized access to data and ensure that use of data is limited to the established public health purpose.

In addition, the Joint Statement calls upon governments to exercise transparency and to fully inform Canadians about the information collected, and its use, access, secure storage and eventual destruction. Given that private sector businesses may be involved in the deployment of information technology in connection with public sector contact tracing efforts, it is important that the products and services developed for this purpose are designed for compliance with the principles outlined in the Joint Statement, applicable laws, and other best practices for personal information processing activities.

Application to Information Technology Development and Marketing Practices

Organizations seeking to develop tracing applications and other similar information technologies should adopt a "privacy by design" framework under which the organization proactively implements privacy controls into the design and development of the information technology and related business practices. Adopting a privacy by design framework is essential to limit the scope of liability and maintain regulatory compliance, particularly where the information technology is to be used in connection with personal information processing activities that are viewed as "extraordinary" by the federal and provincial privacy commissioners.

Further, organizations should ensure that their information technology products and services are prepared in a manner that will allow a public sector institution to conduct a fulsome privacy impact assessment (PIA) with minimal disruption. A PIA is a risk management process that is conducted by public institutions to ensure compliance with the legal requirements (and the institution or program's enabling legislation) and to ensure the potential risks of the personal information processing activities are identified and mitigated. At the federal level, a PIA is required where: (1) personal information is used as part of a decision-making process that directly affects an individual; and (2) the program or activity will have an impact on privacy.[5] It is almost a certainty that a PIA will be required where a federal or provincial institution wishes to engage in contact tracing measures. In fact, a privacy impact assessment is currently underway by the Alberta Privacy Commissioner in connection with the implementation of contact tracing through smartphone technology through ABTraceTogether application.[6]

If an information technology product or service is not designed with the PIA process in mind, the product or

service will be less marketable to public sector institutions. As a result, during the development process it is recommended that organizations should:

- create a clear and accurate data flow diagram demonstrating the collection, use and disclosure of personal information at all stages of processing, with due consideration of the sensitivity of the personal information being processed and the number of people affected;
- consult with stakeholders, partners and governmental authorities to ensure that all privacy risks are identified; and
- consider mitigation strategies when privacy risks are identified that can be incorporated into the design of the information technology. These mitigation measures must be implemented and tracked consistently. Timelines, completion dates and responsibility for implementation should be identified in the PIA.

Taking these proactive steps will help to minimize the privacy issues that may be raised by the applicable privacy commissioner when the client's PIA is formally reviewed.

The Information Technology & Data Privacy Group at Cassels will provide further updates on changes to privacy legislation and guidance in the wake of the COVID-19 pandemic as they become available.

The authors of this article gratefully acknowledge the contributions of articling student Nico Elliott.

---

[1] Office of the Privacy Commissioner of Canada, Joint Statement, "Supporting public health, building public trust: Privacy principles for contact tracing and similar apps" (May 7, 2020), online: <https://www.priv.gc.ca/en/opc-news/speeches/2020/s-d_20200507/#fn1-rf>.
[2] Victoria Gibson, "Ford doesn't rule out using cell data to trace COVID-19 patients", ipolitics.ca (March 16, 2020), online: <https://ipolitics.ca/2020/03/16/ford-doesnt-rule-out-using-cell-data-to-trace-covid-19-patients/>. [Gibson]
[3] Stephanie Hogan, "What is contact tracing? Here's what you need to know about how it could affect your privacy", CBC.ca (May 7, 2020), online: <https://www.cbc.ca/news/canada/coronavirus-covid-19-contact-tracing-app-1.5558512>.
[4] Gibson.
[5] Office of the Privacy Commissioner of Canada, "Expectations: OPC's Guide to the Privacy Impact Assessment Process" (revised March 2020), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/>.
[6] Alberta, "ABTraceTogether", alberta.ca (accessed May 8, 2020), online: <https://www.alberta.ca/ab-trace-together.aspx>.
