Cassels

British Columbia Temporarily Eases Restrictions on the Disclosure of Personal Information Outside of Canada

April 13, 2020

Overview

British Columbia issued a Ministerial Order[1] on March 26, 2020, (the Order) to temporarily modify the *Freedom of Information and Protection of Privacy Act* (FIPPA), which regulates how public bodies handle personal information. The Order was issued in response to the emerging public health needs created by the COVID-19 pandemic in an effort to encourage and facilitate the efficient collaboration and communication among public bodies and healthcare providers in responding to the pandemic. Where the conditions set forth in the Order are met, public bodies are permitted to use third party tools and applications[2] to disclose personal information outside of Canada. We note that the Order grants health care bodies certain additional grounds of disclosure under the Order that are not provided to other public bodies under FIPPA.[3]

The Order is effective until June 2020, unless it is earlier rescinded or extended in full or in part by the Minister of Citizens' Services.

Conditions for the Disclosure of Personal Information Outside of Canada

The Order temporarily permits BC public bodies under FIPPA jurisdiction to disclose personal information outside of Canada through the use of third-party tools and applications in circumstances where the following conditions are met:

- the disclosure is for the purposes that the third-party tools or applications are being used to support and maintain the operation of programs or activities of the public body,
- the third-party tools or applications support public health recommendations or requirements related to minimizing transmission of COVID-19 (e.g., social distancing, working from home, etc.), and
- any disclosure of personal information is limited to the minimum amount reasonably necessary for the performance of duties by an employee, officer or minister of the public body.

In addition to the foregoing, the Order also allows health care bodies to disclose personal information outside of Canada on the condition that the disclosure is:

- necessary for communication with individuals respecting COVID-19,

- in support of a public health response to the COVID-19 pandemic, or
- to coordinate care during the COVID-19 pandemic.

The Use of Third-Party Tools and Applications

The Order allows for third-party tools and applications to be used to facilitate programs and activities in response to public health recommendations or requirements to minimize transmission of COVID-19, such as social distancing and work from home measures.

Before using a third-party tool or application, a public body (which includes any health care body) must be satisfied that the application or tool is reasonably secure in compliance with section 30 of FIPPA. Section 30 of FIPPA requires that the personal information in the custody of a public body or under its control must be protected through reasonable security arrangements to guard against unauthorized access, collection, use, disclosure or disposal. The Order also requires the public body to make all reasonable efforts to remove the personal information collected, used or disclosed through a third-party application as soon as operationally reasonable, and to appropriately retain and manage this information.

Guidelines are still forthcoming from the British Columbia Information and Privacy Commissioner to assist the public sector in selecting the appropriate tools and applications. The implication of this Order for private business is that subcontractors to these public bodies may be able to temporarily offer technical solutions where the data reside outside of Canada.

Storage and Access

Although FIPPA generally restricts storage by a public body of personal information to storage within Canada only, we note that the Order does not address the location of storage of personal information that is disclosed under these new exemptions set forth in the Order. However, section 30.1(b) of FIPPA provides relief in that, if personal information is stored in another jurisdiction for the purpose of a disclosure allowed under FIPPA, the obligation to store such personal information only in Canada does not apply.

Rules Relating to Disclosure of Personal Information In Ontario

In Ontario, the *Personal Health Information and Protection Act, 2004* (PHIPA) governs the collection, use and disclosure of personal health information of individuals. Subsection 50(1) of PHIPA restricts the disclosure of personal health information outside of Ontario unless the individual consents or one of several limited exceptions applies. Although the Information and Privacy Commissioner of Ontario (the IPC), has previously interpreted these provisions as permitting storage of personal health information outside of

Ontario, as of the date of this article, the Ontario government has not yet taken steps to broaden the grounds upon which personal health information could be disclosed outside of Ontario in response to the COVID-19 pandemic. However, in a news release dated March 16, 2020, issued by the IPC, the IPC provided general guidance to organizations regarding the handling of personal information in light of work from home measures currently in effect across the province. According to the IPC, in the exceptional circumstances created by the COVID-19 pandemic "[t]he reasonableness of security and privacy measures has to take into account time-limited, urgent needs."[4]

The IPC further stated that if an organization believes staff need to handle personal information from home in order to provide necessary services efficiently and effectively, the organization should permit such activity and support staff to handle personal information, "within as privacy-protective an environment as they can, given the realities of our current situation." According to the IPC, this may include service professionals especially in health and child protection sectors, sending and receiving information through use of technologies not normally used in the course of business, including phone text, email or messaging services.

Canada's federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*, does not contain guidance on cross-border disclosure of personal information, although this issue was raised in consultations held last year by the Office of the Privacy Commissioner of Canada. (*Please see our previous articles from April 2019, June 2019 and September 2019 discussing this issue*.)

The Privacy Law Group at Cassels will provide further updates on updates 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] Ministerial Order 85/20 (British Columbia Ministry of Citizen's Services), (2020), online: .
[2] In section 4 of the Order, "third party tools and applications" is defined under the Order to include "any software developed and maintained by a third party and which is used to enable communication or collaboration between individuals."
[3] Under Schedule 1 of FIPPA, "health care bodies" include but are not limited to hospitals, provincial mental health facilities, regional health boards and emergency health services, along with the Ministry of Health, the Ministry of Mental Health and Addictions, and the Provincial Health Services Authority.
[4] Information and Privacy Commissioner of Ontario, News Release, "Impact of Covid-19: Notice to the Public and Institutions" (March 16, 2020) online: <www.ipc.on.ca/newsrelease/ipc-closure-during-covid-19-outbreak

---