WeirFoulds LLP

WeirFoulds Technology Insights: "Canadian Privacy & Data Protection Regime"

September 13, 2022

By James G. Kosa and Craig Harasymchuk

Introduction

In the broadest terms, privacy law regulates the collection, use and disclosure of personal information. As such, organizations that collect and use personal information must ensure they comply with the applicable privacy laws in Canada. These laws require organizations to keep an individual's personal information secure and only use the information for the purposes that it was collected, all while keeping in mind the sensitivity of the information.

From the individual's perspective, this means, among other things, an organization must obtain their consent prior to using their information, and further provide an explanation as to why the individual's information is being collected and used.

Canada's "Dual" Type Regime – Public Sector Laws vs Private Sector Laws

It is important to recognize that in Canada, privacy laws can be thought of as being split into two streams: public sector laws and private sector laws.

Public sector laws are those that control the collection, use, and disclosure of personal information by the federal, provincial, and municipal governments. They are the laws that restrict what the government can do with collected personal information, as well as provide an avenue for its citizens to obtain or request information from the government. These laws include the *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31 ("**FIPPA**"), *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56 ("**MFIPPA**"),and the *Privacy Act*, R.S.C. 1985, c.P-21. FIPPA and MFIPPA are both provincial legislation in Ontario, while the *Privacy Act* is federal legislation.

Private sector laws are those which regulate how non-governmental organizations can collect, use, and disclose personal information for their legitimate business purposes. In this space, the federal government enacted the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("**PIPEDA**"). PIPEDA applies in all provinces except for Alberta, British Columbia, and Quebec, which have enacted their own acts that essentially supersede PIPEDA. In 2004, the Ontario government enacted the *Personal Health Information Protection Act*, 2004, S.O., c. 3, Sched. A ("**PHIPA**"), which is specific to the collection of personal information in the health care sector.

But first, what is "personal" information anyways?

"Personal" information has been defined very broadly across the relevant legislation, but in essence, it means "recorded" information about an "identifiable individual." However, a person is only "identifiable" where it is reasonable to expect that an individual may be identified if the information is disclosed. Some relevant examples include race, religion, ethnic origin, sex, sexual orientation, marital

status, family status, education, medical, criminal, employment history, address, telephone number, and the list goes on. As such, when an organization is determining whether the information it has requested from an individual is "personal," it should put significant thought and care into whether an individual can be *identified* by the provided information.

The Introduction of Bill C-11 and its Impacts

On November 17, 2020, the Federal Government introduced Bill C-11 with the intention to bring Canada in line with more stringent privacy protections that are provided in other jurisdictions, for example, in the European Union under its General Data Protection Regime. Bill C-11 contains two parts. Part 1 would enact the *Consumer Privacy Protection Act* ("**CPPA**") and Part 2 would enact legislation to establish a Personal Information and Data Privacy Tribunal.

In general, Bill C-11 would make it easier for individuals to access their data, provide greater protections, create a new right of "data portability", and significantly increase fines. For example, for a breach of privacy, the fine could be the greater of $10,000,000 or 3% of the organization's global revenue. But it doesn't stop there. The penalty for obstructing a Commissioner's investigation could be the lesser of $25,000,000 or 5% of the organizations global gross revenue.

Key Changes in Bill C-11 that Companies Should Prepare for

The CPPA will require an individual's consent before or at the time their personal information is collected and the use of plain language. Organizations *must* make available, in plain language, explanations to its policies and obligations in relation to an individual's personal information. For organizations that use algorithms to assist or replace human judgement, this also means providing an explanation as to how the algorithm came to its conclusions when such an explanation is requested by an individual.

Furthermore, organizations will be required to dispose of the information as soon as reasonable and individuals will also be allowed to request their information be disclosed to a third party designated organization.

The Ontario White Paper and its Vision for the Future

The Ontario Government believes that Bill C-11 has weaknesses which should be improved upon and envisions passing a law that will strengthen those weaknesses. The Ontario Government's thoughts about such weaknesses were captured and released in its Modernizing Privacy in Ontario – White Paper. It believes that Bill C-11's framework could allow organizations to collect and use citizens' data for commercial interests without their knowledge. It also does not provide adequate protection for children and youth, and its digital rights to not go far enough to protect individuals from new risks.

Thus, Ontario envisions itself passing legislation which would strengthen reforms in the following areas: automated decision making; consent and other lawful uses of personal data; transparency; protection of children and youth; regulatory oversight; and support for Ontario innovators.

Conclusion

For companies that routinely request and obtain personal information, it would be prudent for them to turn their mind to these upcoming issues to be adequately prepared for the future. This may be especially true for large companies where the implementation of such policies and procedures may be difficult on a large scale, and small companies where the cost of compliance may be an issue.

For more information or inquiries:

James G. Kosa

Toronto
416.947.5043

Email:
jkosa@weirfoulds.com

James Kosa is a partner at WeirFoulds with a practice focused on information technology and intellectual property law. He is the Co-Chair of the firm's Technology & Intellectual Property and Privacy & Access to Information Practice Groups, and Co-Chair of the Blockchain and Digital Assets Practice Group.

WeirFoulds LLP

www.weirfoulds.com

Toronto Office
4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110
Fax: 416.365.1876

Oakville Office
1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110
Fax: 905.829.2035