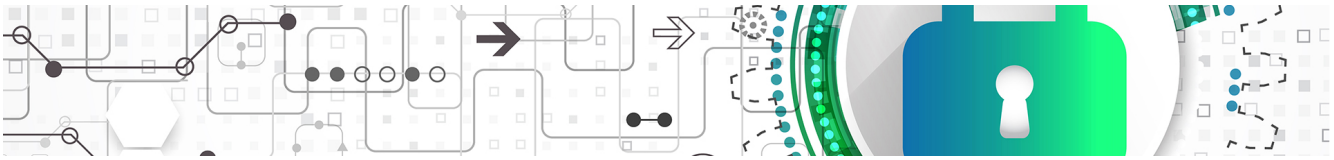

Wait… There's More Than Just a Privacy Policy? Things Start-ups Should Know About Privacy Law in Canada

February 4, 2019

By Amanda Branch

Pop quiz.

Data is:

a. The world's most valuable resource,
b. The new oil, or
c. The new bacon.

No matter how you describe it, data is extremely important to organizations. With smart technology and connected devices all around us, consumers are increasingly aware of the importance of privacy and protection of personal information. New technologies give organizations an almost unlimited capacity to collect vast amounts of personal information, analyze it, use it and communicate it to others; however, organizations must be careful to do so in a way that is compliant with privacy legislation.

Read on to learn what start-ups should know about privacy law in Canada (spoiler alert: yes, there is more than just a privacy policy!).

Starting with the basics

The *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") applies to private sector organizations in Canada that collect, use, or disclose personal information in the course of commercial activity, except where that activity takes place entirely within a province with "substantially similar" legislation (currently Quebec, Alberta and British Columbia).

What is "personal information"?

Personal information is any "information about an identifiable individual". This is a very broad definition and can include things like name, address, government-issued identifiers, health information and medical records, financial information and biometric data.

What you should know

1. Do I need a privacy policy?

Yes, if your organization is subject to PIPEDA, then you are required to develop and implement policies and practices and you must make these policies readily available to consumers.

2. What's so important about consent?

Consent is an important part of Canada's private sector privacy legislation. Consent is considered valid only if meaningful, that is, if it is reasonable to expect that individuals to whom a business' activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure to which they are consenting.

As of January 1, 2019, the Office of the Privacy Commissioner of Canada (the "**OPC**") began applying its Guidelines for obtaining meaningful consent (the "**Consent Guidelines**"). You can read more about the guidelines here.

3. We have a privacy policy on our website. Our work here is done, right?

Wrong. A privacy policy is just a part of your obligations under privacy law. In addition to external documents, businesses must develop and implement internal policies and procedures to protect the personal information handled by employees. These policies should address, for example, your internal practices for the collection, handling and storage of personal information and how you will respond to access requests or complaints.

Once you have these policies, you need to do more than file them away never to be seen again. Policies and practices should be regularly reviewed, audited and updated.

4. We've collected a bunch of personal information that we're going to keep forever. Is that okay?

Nope. Generally speaking, it is not appropriate to keep personal information indefinitely. Data should be retained only as long as required to satisfy the stated purpose at the time of collection. Organizations should have policies and procedures in place for the retention and destruction of personal information and once the information is no longer required, it should be destroyed, erased or rendered anonymous.

(Speaking of inappropriate data practices, as of July 1, 2018, the OPC has been applying its Guidance on inappropriate data practices: Interpretation and application of subsection 5(3). Read more about the guidance here.)

5. Uh oh, we just had a breach. Now what?

Hopefully you planned ahead and have a data breach response plan in place.

As of November 1, 2018, the mandatory breach notification requirements under PIPEDA came in to force. Pursuant to the legislation, if an organization suffers a breach of security safeguards that gives rise to a "real risk of significant harm", the organization must (i) report the incident to the Office of the Privacy Commissioner of Canada (the "OPC"); (ii) notify affected individuals; and (iii) notify any other third party organizations or government institutions that are in a position to mitigate the risk of harm to affected individuals. These notifications must be made as soon as feasible after the organization determines that the breach has occurred.

If you need help, look no further. The OPC recently released its breach guidance, "What you need to know about mandatory reporting of breaches of security safeguards" and we have broken it down for you here.

This article was also published in the IICIE blog.