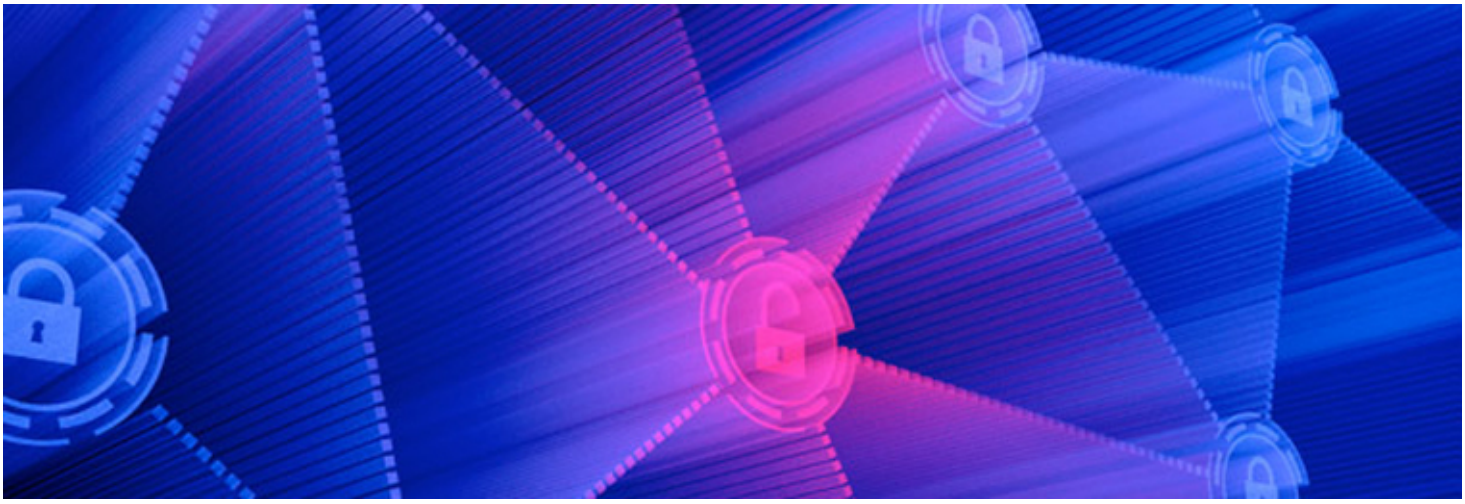

Canada's PIPEDA: consultation opportunity for data breach reporting regulations

Data Protection, Privacy and Security Alert

5 MAY 2016
By: Tamara Hunter | Jim Halpert

The Canadian government continues to move forward with the regulation development process relating to data breach reporting.

Innovation, Science and Economic Development Canada recently issued a discussion paper regarding the development of data breach notification and reporting regulations under the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), and has invited interested stakeholders to provide written comments and responses by **May 31, 2016**.

This is the latest step in Canada's upgrading of *PIPEDA*. New Canadian breach notification provisions were released in June 2015, as part of Canada's *Digital Privacy Act.* However, these provisions are not yet in force. They will only become law after the release of regulations that will provide more detailed direction on the content, form and manner of notification.

Innovation Canada's invitation provides an opportunity for stakeholders to potentially influence the content of the breach notification regulations. As *PIPEDA* is not sector-specific, the regulations apply to a variety of organizations.

Current breach notice law and practice in Canada

Among other things, *PIPEDA* governs the ways private sector organizations subject to *PIPEDA* may collect, use and disclose personal information in the course of commercial activity. The *Digital Privacy Act* amended some aspects of *PIPEDA*, including introducing a new data breach notification requirement (which is not yet in force).

As mentioned, because the data breach regulations still have not been released, Canada's *PIPEDA* breach notice requirements have not taken effect. However, the Privacy Commissioner of Canada has, for some time, encouraged organizations to voluntarily report material information security breaches to the Commissioner (and to notify affected individuals where they face a risk of harm) and provides a Privacy Breach Incident Report Form on its website for that purpose. The Office of the Privacy Commissioner of Canada also monitors breaches of which it is aware and investigates complaints it receives regarding information security breaches.

Alberta is currently the only province in Canada to have generally applicable mandatory data breach reporting requirements for all private sector organizations. (However, some provincial health privacy statutes do contain breach reporting requirements for the healthcare sector). The Alberta Information and Privacy Commissioner routinely posts decisions on its website regarding whether information security breaches reported by named organizations meet the Alberta *Personal Information Protection Act* risk threshold of "a real risk of significant harm" to affected individuals. These Alberta Commissioner reports set out a description of the incident, the nature of potential harm to individuals arising from the incident and any steps taken by the organization to reduce the risk of harm (including any pro-active notification of individuals by the organization).

Class actions for information security and other privacy breaches are becoming more prevalent in Canada, and it can be expected that mandatory reporting requirements for information security breaches will lead to increased class actions in this area. In Canada, privacy breach class actions have been certified, in some circumstances[1], even where actual financial harm or pecuniary loss cannot be proven. The extent to which Canadian privacy breach class actions are ultimately successful on their merits remains to be seen.

The *PIPEDA* breach notice regime

When the breach notification provisions in *PIPEDA* do come into effect, they will require organizations to report to the Privacy Commissioner of Canada (and, generally, to affected individuals and certain third parties) any breach of security safeguards which meet the risk threshold of being reasonably believed to create "a real risk of significant harm to an individual".

In assessing the potential for significant harm, *PIPEDA* will require organizations to consider "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property".

The *PIPEDA* provisions will also require that the notification:

1. "contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm", and that the notification be made "as soon as feasible after the organization determines that the breach has occurred"; and
2. be "conspicuous" and given directly to the individual, except when the breach notification regulations authorize indirect notification in the circumstances. The *PIPEDA* breach notification provisions leave the precise form and manner of the notification to be specified in the regulations.

Organizations that knowingly violate the breach notification requirements may face fines of up to $100,000 (US $78,615) per violation.

The ministry consultation: questions for stakeholder input

The discussion paper does not contain draft breach notification regulations, nor does it set out the position of Innovation Canada on what should be contained in regulations. Rather, the discussion paper sets out a series of 26 questions and solicits stakeholder input and views on those questions. For example, the discussion paper has posed questions such as:

- Is it necessary to identify additional risk-assessment factors in the regulations or are the factors listed in the legislation (i.e. sensitivity and probability of misuse) sufficiently clear?
- Should the regulations specify that the risk to individuals can be presumed to be low in circumstances where appropriate encryption has been used?
- Should reports to the Commissioner contain an assessment by organizations of the types of harm that may result from a breach as well as the likelihood of that harm occurring?[2]
- Should the regulations require organizations to update the Commissioner in circumstances where the information provided in the original report is discovered to be inaccurate, incomplete or has changed?
- Is it necessary for the regulations to identify specific information to be included in notifications to individuals or is the legislation sufficiently clear?
- What methods of communication should be permitted for direct notification to individuals?
- In what circumstances should organizations be permitted to indirectly notify individuals of a data breach?

Next steps

Following the consultation process arising from the discussion paper, the Canadian government will prepare and publish draft regulations for public comment and consultation. While the Canadian government has not specified an expected time frame for publishing draft regulations, we would not expect such draft regulations to be published until late 2016 at the earliest or, more likely, in 2017.

As stated above, the regulations will apply to a broad variety of organizations. Stakeholders that wish to take part in the comment process regarding the content of the breach notification regulations should act now.

DLA Piper has significant experience with data breach notice in Canada and is following the development of regulations closely. Organizations that would like assistance in commenting on the questions raised by the discussion paper on the *PIPEDA* Security Breach Notification Regulations, or in preparing for or responding to an information security breach situation, should please contact any of the authors.

For more details, please see our July 2015 article in the Bloomberg BNA World Data Protection Report on Canada's *Digital Privacy Act* which highlighted changes to Canada's *PIPEDA*.

---

[1] For example, where the underlying common law or statutory cause of action does not require proof of damages.

[2] We note that a requirement for such an assessment may tend to discourage reporting of information breaches by organizations, given that such an assessment may be used against an organization in a subsequent class action. Some may take the view, however, that without a requirement for such an assessment, the regulations may not be consistent with the *PIPEDA* requirement for notification to "contain sufficient information to allow the individual to understand the significance to them of the breach…".

AUTHORS

Tamara Hunter
Associate Counsel
Vancouver | T: +1 604 687 9444
tamara.hunter@dlapiper.com

Jim Halpert
Partner
Washington, DC | T: +1 202 799 4000
jim.halpert@dlapiper.com