Federal Breach Notification Rules Finalized; In Force November 2018

April 16, 2018

David Elder, Rona Ghanbari

Nearly 3 years after passing amendments to Canada's federal private sector privacy law to include mandatory breach notification and record-keeping requirements, the Government has finalized some related regulations and announced that the new obligations will come into force on November 1, 2018.

As of that date, organizations that are subject to the *Personal Information and Electronic Documents Act* (*PIPEDA*) will be required to both notify affected individuals and report to the Office of the Privacy Commissioner of Canada (OPC) any breach of security safeguards with respect to personal information under the organization's control, if it is reasonable in the circumstances to believe that the breach creates "a real risk of significant harm to an individual. " Both the report and the notifications must be given as soon as feasible after the organization determines that a breach has occurred.

Organizations will also be required to maintain records of every breach of security safeguards involving personal information under their control – even those that do not meet the "real risk of significant harm" threshold, and which would not require notification to affected individuals or reporting to the OPC.

Background

In June 2015, the *Digital Privacy Act* introduced several changes to Canada's private sector privacy legislation, PIPEDA, including the introduction of mandatory data breach reporting requirements. However, unlike some of the other amendments to the law contained in the Digital Privacy Act (which came into force with the passage of that Act), the breach notification reporting and notification obligations were not proclaimed in force, pending the adoption of regulations providing further details with respect to the obligations.

In September, 2017, the government published proposed Breach of Security Safeguards Regulations to bring these provisions into force. The final version of these Regulations was published on April 18th, along with a regulatory impact assessment that provides some of the rationale behind the government's approach to the Regulations.

The final version of the Regulations does not differ substantively from the draft regulations, but does include a number of revisions that generally provide more flexibility to organizations.

The coming into force of PIPEDA's data breach provisions will mean that data breach reporting and notification obligations for private sector organizations will now exist in all Canadian provinces and territories except for British Columbia and Québec, each of which has its own, provincially-enacted private

sector privacy law. The Province of Alberta has had mandatory data breach reporting requirements in its private sector privacy law since 2010. Several of the provinces have also enacted health sector privacy laws that require breach notification.

The New Obligations

PIPEDA itself sets out the main reporting and notification requirements, including defining what constitutes significant harm, and what factors are relevant to determining whether a breach creates a real risk of such harm.

The term “significant harm” is defined broadly, to include a wide range of harms: bodily harm; humiliation; damage to reputation or relationships; loss of employment, business or professional opportunities; financial loss; identity theft; negative impact on credit records; and damage to or loss of property. In assessing the risk of harm, organizations must consider a range of factors, including the sensitivity of the personal information involved and the probability that the personal information has, or will, be misused.

Somewhat unique among breach notification laws, PIPEDA contains a broad requirement for an organization to also notify any other organization or government institution of a breach, if such organizations or institutions may be able to reduce the risk of harm or mitigate the harm.

For their part, the Regulations contain more detailed guidance respecting the following:

1. **The information that must be contained in the written breach report to be provided to the OPC**.
   The information to be provided in the report comprises the key details that one would expect to be included in such a report: timing, personal information involved, number of individuals affected, steps taken to reduce harm, plans for notification, etc. – and the required details are generally consistent with other data breach reporting regimes. Unlike the draft regulations, the final version recognizes that in a data breach situation, an organization typically becomes aware of the details piece by piece, over a period of time. Accordingly, the Regulations explicitly contemplate that organizations may submit new information to the OPC at any time after the original report. Reports may be sent by any secure means of communication.

2. **The information that must be contained in the breach notification to be provided to affected individuals.**
   Again, the Regulations require what one would expect to be included in a notification to affected individuals: a description of the circumstances, timing, personal information involved, steps taken to reduce harm, steps individuals could take to further reduce risk of harm, etc. Of course, the notice must contain contact information that the individual can use to obtain further information; however, unlike the draft regulations, the final version is not prescriptive about the type of contact information that may be required, giving organizations to choose the method that makes the most sense in their operational context.

3. **The manner in which direct notification must be given to affected individuals.**
   The Regulations allow for notification in person, or by telephone, mail or email, or any other form of communication that a reasonable person would consider appropriate in the circumstances. The earlier version of the Regulations was more prescriptive in this regard.

4. **The circumstances in which indirect notification may be given to affected individuals, and the form and manner for such notification.**
   PIPEDA generally requires direct notification to affected individuals, but provides for the possibility of indirect notification in prescribed circumstances. The Regulations allow for indirect notification where either:
   - Giving direct notification would be likely to cause further harm to the affected individual
   - Giving direct notification would be likely to cause undue hardship for the organization

   Indirect notification must be given by public communication or a similar measure that could reasonably be expected to reach the affected individuals, providing organizations with greater flexibility than the earlier draft regulations, which allowed for only advertisements or website notices.

   The possibility of indirect notification may be particularly relevant in cases where the risk of harm relates primarily to damage to reputation through public exposure, since in such cases, the sending of the notification itself may provide further exposure of the activity or circumstance giving rise to that risk.

   With respect to “undue hardship” to an organization, this exception is expanded from the previous draft, which referenced only prohibitive cost to an organization.

5. **The period for which organizations must retain records of every breach of security safeguards, and general guidance as to the content of these records.**
   The Regulations provide that records of breaches need only be retained for a period of 24 months after the breach occurred, somewhat limiting the administrative burden on organizations. However, the Regulations do not provide much additional guidance re the required content for such records, providing only that they must contain “any information that enables the Commissioner to verify compliance” with PIPEDA’s data breach reporting requirements.

Challenges

Data breach reporting under PIPEDA has been a long time in coming, and the inclusion of mandatory breach reporting provisions in the law was and is largely supported by Canadian businesses. Particularly for global businesses, which already face mandatory breach reporting obligations in many other jurisdictions, including the EU and most states in the U.S., compliance with the new Canadian federal breach reporting requirements should not prove to be particularly difficult, although we expect some initial uncertainty about how the “real risk of significant harm” threshold will be interpreted and operationalized.

Perhaps what may create more difficulties for business will be the legal requirement to report breaches to other organizations that may be able to reduce harm, as it may not be entirely clear in all cases to which organizations a business might be compelled to report. For example, in cases where identity theft may be part of the risk of harm, will business be required to disclose breaches directly to credit reporting agencies, financial institutions, etc.? If they are, what are such organizations expected to do? Such third parties are under no legal obligation under PIPEDA to take any action respecting a breach reported to them, nor are they required not to disclose the details of any breach communicated to them.

Finally, we expect that many organizations will struggle with the new obligation to keep records of “all breaches of security safeguards,” since there is no threshold of materiality for this requirement: even trivial breaches concerning a single individual require that record be kept. For many businesses, such as retail businesses with many customer-facing employees, operationalizing this new requirement may be difficult. Moreover, the new record keeping requirement, like the data breach reporting and notification provisions, is one of the few provisions of PIPEDA with respect to which non-compliance constitute an offence.