Published on *The National Law Review* https://natlawreview.com

Canada's New Data Breach Notification Law

Article By:

Anjali C. Das

For several reasons, 2018 will go down in legal history as the Year of Global Privacy Legislation. In February of this year, the breach notification amendments to Australia's Privacy Act of 1988 went into effect. On May 25, 2018, the unprecedented, sweeping European Union (EU) privacy law known as the General Data Protection Regulation (GDPR) went into effect; it imposes stringent requirements on companies to safeguard the personal information of EU citizens. One month later, on June 28, 2018, the State of California passed the **California Consumer Privacy Act of 2018**, which adopts strict parameters on the collection, use and sale of personal information of California residents. Later this year, on November 1, 2018, the long-awaited amendments to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) will go into effect. These amendments and regulations related to PIPEDA, which are the subject of this article, impose new mandatory notification obligations on companies in the event of a breach involving the personal information of Canadians.

PIPEDA

Canada enacted the nation's privacy law for the private sector, PIPEDA, on April 13, 2000. The stated purpose of the Act was to "govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information." On June 18, 2015, the Digital Privacy Act amended certain provisions of PIPEDA, including the introduction of a mandatory data breach notification requirement similar to those that currently exist in the United States. However, the implementation of PIPEDA's breach notification requirements was temporarily on hold, pending the creation of new Breach of Security Safeguards Regulations (Regulations). The final version of these Regulations was published on April 18, 2018. The new data breach reporting requirements contained in Division 1.1 of PIPEDA along with the related Regulations will go into effect on November 1, 2018.

Entities Subject to PIPEDA

PIPEDA generally applies to non-federally regulated private sector organizations in Canada that collect, use and disclose personal information (typically of customers) in the course of commercial for-profit activities. PIPEDA also applies to personal information of employees of federally regulated businesses in Canada, such as banks, airlines and telecommunications companies.

However, certain Canadian provinces that have enacted private sector privacy laws deemed to be "substantially similar" to PIPEDA may be exempt. To date, there are a limited number of provincial laws that have mandatory breach notification requirements. This includes Alberta's Personal Information Protection Act (PIPA) in addition to various provincial laws adopted by Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia that protect the privacy of personal health information. For instance, Alberta's PIPA requires an organization to provide notice of a breach to the Privacy Commissioner without unreasonable delay if there is a "real risk of significant harm" to an individual. In addition, notification should be provided to individuals as soon as possible to avoid or mitigate harm.

Notwithstanding, PIPEDA still applies to all inter-provincial and international commercial transactions involving the personal information collected, used or disclosed by organizations in Canada.

Moreover, it is significant to note that PIPEDA may have extraterritorial application to companies located outside Canada's borders. The statute itself is silent with respect to the Act's territorial reach. However, Canadian courts have held that PIPEDA has extraterritorial application to a foreign organization that has a "real and substantial link" to Canada. For instance, last year a Canadian court held that a foreign-based website operator was subject to PIPEDA. The court considered a number of factors to establish a sufficient connection between the company and Canada, including the operation of a website targeting Canadians that published their personal information. As such, any organization that conducts business in Canada and/or collects, uses or discloses information concerning Canadians may be subject to PIPEDA.

New Data Breach Notification Requirement

Canada's new mandatory breach notification law applies to situations involving a "breach of security safeguards." PIPEDA defines this as the "loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards."

PIPEDA broadly defines "personal information" as "information about an identifiable individual." In other words, it is information that can be linked to a specific individual. The Office of the Privacy Commissioner of Canada has listed various examples of personal information that may include (but is not limited to):

- Race, national or ethnic origin
- Religion
- Age, marital status
- Medical, education or employment history
- Financial information
- DNA
- Social insurance number or driver's license.

As explained in the Government of Canada's Regulatory Impact Analysis Statement (Impact Statement), which accompanied the draft Regulations, one of the key objectives of the new law is to "ensure that all Canadians will receive consistent information about data breaches that pose a risk of significant harm to them." Subsection 10.1(3) of PIPEDA further states that "an organization shall notify an individual of any breach of security safeguards involving the individual's 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 the individual."

Subsection 10.1(7) of PIPEDA defines “significant harm” to include “bodily harm, humiliation, damage to reputation or relationships, loss of employment, [loss of] business or professional opportunities, financial loss, identity theft, negative effects on credit record and damages to or loss of property.” Subsection 10.1(8) of PIPEDA identifies several factors to determine whether an individual may be subjected to “real risk” of significant harm in the event of a breach, including, but not limited to, (1) the sensitivity of the personal information involved in the breach and (2) the probability that the personal information has been or will be misused.

As explained in the Impact Statement, the organization must conduct a “risk assessment” to determine whether the breach posed a “real risk of significant harm” based on the surrounding circumstances. Even if the organization determines that there is no significant risk of harm that warrants notification, a well-documented risk assessment can protect the organization if there are any subsequent inquiries regarding the breach.

Contents of Individual Notice

Subsection 10.1(4) of PIPEDA states that the notice should contain sufficient information to enable 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.” The Regulations further state that notice to affected individuals *must* contain the following information:

- A description of the circumstances of the breach
- The day on which the breach occurred (or approximate time frame if the exact date is not known)
- A description of the personal information that was the subject of the breach
- A description of the steps taken by the organization to reduce or mitigate the risk of harm
- A description of the steps the affected individuals can take to reduce or mitigate the risk of harm
- Contact information for the affected individual to obtain additional information about the breach.

Timing of Individual Notice

Subsection 10.1(6) of PIPEDA states that notice shall be provided “as soon as feasible” after the organization has determined that a breach has occurred.

Form and Manner of Individual Notice

The Regulations provide for either “direct” or “indirect” notification to individuals. For purposes of direct notification, the organization must give affected individuals notice “in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances.”

The Regulations further state that an organization may give indirect notification of a breach in any of the following circumstances: (1) direct notification would be likely to cause “further harm” to the affected individual, (2) direct notification would be likely to cause “undue hardship” for the organization or (3) the organization does not have contact information for the individual. While the Regulations do not specify the means of indirect notification, some examples may include a public communication, such as an advertisement or conspicuous posting on the organization’s website.

Notice to the Privacy Commissioner

Subsection 10.1(1) of PIPEDA also requires an organization to provide notice of a breach to the Privacy Commissioner "if it is reasonable … to believe that the breach creates a real risk of significant harm to an individual." In other words, if the organization determines that notice to the affected individuals is warranted, notice also must be provided to the Commissioner.

The Regulations state that notice to the Commissioner *must* contain the following information (which is similar to the information contained in the notice to individuals described above):

- A description of the circumstances of the breach and cause, if known
- The day on which the breach occurred (or approximate time frame if the exact date is not known)
- A description of the personal information that was the subject of the breach
- Number of affected individuals
- A description of the steps taken by the organization to reduce or mitigate the risk of harm
- A description of the steps taken by the organization to notify affected individuals
- The name and contact information of a person who can answer further questions by the Commissioner concerning the breach.

The Regulations further provide that the organization can supplement its initial notice to the Commissioner if new information becomes available.

Notice to the Commissioner may be provided by any "secure" means of communication, which is not defined in the Regulations but would likely encompass encrypted communications.

Organizations' Duty to Keep Records of All Breaches

Last, but not least, Subsection 10.3(1) of PIPEDA requires an organization to "keep and maintain a record of every breach of security safeguards involving personal information under its control." The Privacy Commissioner may request copies of all such records at any time. The Regulations further state that the organization must maintain records of all breaches for at least 24 months following the date it determined that a breach occurred. According to the Impact Statement, the purpose of this record-keeping requirement "is to facilitate oversight of organizations' breach reporting and notification obligations by the Commissioner. This, in turn, will [presumably] encourage better data security practices by the organizations."

Conclusion

In summary, effective November 1, 2018, all organizations conducting business in Canada that experience a breach of security safeguards exposing personal information of Canadians will be required to (1) provide affected individuals with mandatory notification if the breach poses a "real risk of significant harm," (2) provide notice to the Privacy Commissioner of such breaches and (3) maintain internal records documenting all known breaches.

As explained in the Impact Statement, the mandatory breach notification under PIPEDA provides a minimum standard for notification and consistency in reporting that has previously been absent outside of Alberta and the health sector in certain provinces. Moreover, Canada's new notification requirements are consistent with those of the country's major trading partners, including the EU. In

particular, the Government of Canada notes that “PIPEDA is currently deemed to provide an essentially equivalent level of privacy protection to the EU, which allows for the free flow of personal information from the EU to Canadian organizations.”

National Law Review, Volume VIII, Number 204