David Young Law
Compliance Bulletin
July 2015

Federal Privacy Law Amended –Breach Reporting and Other Changes Affecting Organizations

David Young

After ten years of study and five years of on-again off-again legislative debate, Parliament has adopted significant amendments to the federal privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The *Digital Privacy Act*, passed by the Senate on June 18, 2015, contains important changes to the privacy rules affecting organizations. While including significant new obligations – such as a mandatory requirement for breach reporting – the amendments also include rules that facilitate many day-to-day business practices that were not addressed when PIPEDA first came into law 15 years ago. These facilitating rules, seen as long overdue, will bring PIPEDA into line with the existing privacy regimes in Alberta and B.C.

Breach reporting and notification

The most significant change is the new requirement for organizations that suffer a privacy breach to: (a) report the breach to the federal Office of the Privacy Commissioner (OPC) and (b) notify all affected individuals, *in both instances, if it is reasonable in the circumstances to believe that the breach has a real risk of significant harm to one or more individuals*.

The legislation contains a non-exhaustive definition of "significant harm". Essentially, "significant harm" includes physical harm, humiliation, reputational harm, loss of employment, business or professional opportunities, and harm to a credit record.

The law also includes a non-exhaustive listing of factors relevant to determining whether a breach creates a "real risk", which list can be extended by regulation. Specifically stipulated as factors relevant to risk are: (a) the sensitivity of the affected personal information and (b) the probability that the information has been, is being or will be misused.

In addition to reporting breaches to the OPC and notifying affected individuals, organizations are required to notify other organizations (such as credit bureaus) and government bodies if they believe that such third parties may be able to reduce the risk or mitigate the harm that could result. Additional requirements for third party notifications may be prescribed by regulation.

In all cases, reporting and notification of breaches must be made as soon as feasible once the organization determines that a breach has occurred.

David Young Law • Hudson's Bay Centre, Suite 3500, 2 Bloor Street East, Toronto, ON M4W 1A8
T. 416-968-6286 • M. 416-318-5521
Privacy and Regulatory Law Counsel • davidyounglaw.ca

Regulations will be issued setting out the prescribed form and content of breach reports to be made to the OPC. For an idea of what may be required in such reports, reference may be had to the regulation issued under Alberta's *Personal Information Protection Act* (PIPA), which has required such reporting since 2010. Notifications to affected individuals must contain sufficient information to allow the individuals to understand the significance of the breach and to take steps where possible to reduce the risk of harm or to mitigate it. Regulations may be issued stipulating other information to be included. Notifications must be conspicuous and delivered directly to affected individuals in the manner and form set out in the regulations, except in those circumstances, specified by regulation, when notification may be given in another manner, such as publication in media.

Finally, organizations will be required to maintain *a record of all privacy breaches* (including those not requiring reporting and notification, as not meeting the test of real risk of significant harm) and shall provide a copy of such record to the federal Privacy Commissioner on request. Regulations may be issued stipulating the form and level of detail required to be kept in such record, as well as the required retention period.

In addition to these new compliance requirements for breach response, the amendments make it an offence, punishable by a fine of up to $100,000 for each incident, for an organization to knowingly contravene the requirements.

Impact on organizations

As noted above, numerous provisions of the new breach rules will be detailed in regulations. Pending issuance of these regulations, the new breach rules are not yet in force. A period for public commentary and finalization of draft regulations may be provided. However organizations should not wait until the regulations are issued to initiate adjustments, where required, in their internal procedures to respond to the anticipated new requirements. Furthermore, even though the amendments are not yet in force, organizations should consider adopting, voluntarily, reporting and notification procedures in line with the anticipated requirements. Reference to the OPC's existing guidance regarding notification and reporting is available on its website.

The new breach provisions will require organizations to have in place internal procedures to ensure that breaches are identified and reported internally at the earliest possible time as well as response protocols to ensure appropriate measures are taken in connection with any breach. An important purpose of these procedures and protocols is to ensure that the new mandatory reporting, notification and record-keeping requirements are complied with.

In addition to the likely heightened compliance burden imposed by the new breach response rules, organizations may face added risks and challenges. For example, exposure to class action litigation may be increased by the notification requirement and information discoverable in such litigation may be facilitated through the new record-keeping requirements. It will be incumbent upon an organization to

ensure that its procedures effectively address reduction or mitigation of potential harm to individuals and minimization of risk to the organization.

A further impact of the new breach provisions may be noted. While not statutorily required in provincial jurisdictions having privacy laws with less stringent requirements (such as Ontario's personal health information protection law and Quebec's private sector privacy law), it can be anticipated that the new PIPEDA rules may become a best practice recognized by regulatory authorities and the courts in those jurisdictions, and may serve as a precedent for amendments to those laws.

Heightened consent requirement

A further, potentially onerous, requirement for organizations under the PIPEDA amendments is a stipulation that consent to collect, use or disclose personal information is only valid if it is reasonable to expect the affected individual to understand the nature, purpose and consequences of that consent.

It is not clear the extent to which this new requirement changes the existing stipulation under PIPEDA's Consent Principle (section 4.3.2 of Schedule 1), that organizations must make a reasonable effort to ensure that individuals are advised of the purposes for which their personal information will be used and to state such purposes in a manner that individuals can reasonably understand how that information will be used or disclosed. However, the new stipulation clearly imposes additional criteria for effective consent, particularly where obtained from vulnerable individuals, or children. In addition, consents obtained from large numbers of individuals through the use of standard forms (such as customers or employees) may be subject to scrutiny and challenge if it can be shown the new criteria are not satisfied.

All organizations should undertake an immediate review of their consent forms, privacy documentation including online privacy consents, and their procedures to ensure that the consents they obtain will remain valid.

Other amendments

While, as noted, the PIPEDA amendments stipulate new or heightened compliance requirements for organizations, the legislation also includes a number of important exceptions to PIPEDA's consent rules which are consistent with the Alberta and British Columbia private sector privacy laws (*Personal Information Protection Acts*) and which facilitate day-to-day business practices. These amendments are considered long overdue.

In summary, these facilitating amendments enable organizations to:

(i) disclose personal information to other organizations in connection with investigations (such as relating to a breach of law or fraud);

(ii) stipulate that for employees governed by PIPEDA (i.e. those employed by "federal works"), organizations may simply provide notice of collection, use or disclosure of personal information instead of requiring consent;

(iii) deal with, without consent, personal information generated by an individual in connection with his or her work, business or profession ("work product information"); and

(iv) collect, use and disclose personal information in connection with transactions involving a purchase and sale of a business provided that the primary purpose or result of such transaction does not focus on personal information.

In addition, a broader definition of "business contact information", stipulated as an exception to the application of PIPEDA, has been adopted. The new definition means that any information used for the purposes of communicating or facilitating communication with an individual in relation to their employment, business or profession is excluded from the application of the law. The definition is stated in general terms and significantly includes, by way of example, work electronic addresses which previously had been determined not excluded under PIPEDA as originally enacted.

Other exceptions to the consent requirement address disclosure of personal information to government or next of kin in cases of financial abuse, or in the event of an injury or death of an individual.

Finally, witness statements obtained outside of formal litigation procedures, such as in connection with assessing an insurance claim, are now exempt from the consent requirements.

Conclusions

The *Digital Privacy Act* really should be entitled "the PIPEDA Amendment Act" because it addresses diverse amendments to that law, many considered long overdue, as opposed to digital privacy per se.

The amendments impose significant new requirements on organizations, primarily in connection with breach response and valid consent. However the law also contains a number of refinements that facilitate organizations in carrying out their day-to-day business operations without additional concerns that these operations may run afoul of the law.

For more information please contact:

David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.