JULY 2, 2015

Digital Privacy Act

Author: Elliot A. Greenstone

On June 18, 2015, the *Digital Privacy Act* (Act) came into effect, amending the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and implementing significant amendments to the private sector privacy regime. The amendments include the expansion of the Privacy Commissioner's (Commissioner's) powers, a consent-and-disclosure exception for certain business transactions and mandatory data-breach notification rules. All the amendments are in effect immediately except those relating to data-breach notification, which will come into force once regulations are complete.

Extension of Privacy Commissioner's Powers

The Commissioner can now enter into compliance agreements with an organization that the Commissioner believes has committed, is about to commit or is likely to commit, an act or omission that contravenes PIPEDA.

The Commissioner now also has the power to disclose any private information obtained while performing or exercising his or her duties if it is in the public interest to do so. The Commissioner may also disclose to a government institution any information obtained in a report regarding a breach of security safeguards if he or she reasonably believes that the information could be useful in investigating a contravention of federal or provincial laws that has been or is about to be committed.

Business Transaction Exception

A long-awaited amendment is the business transaction exception, which brings PIPEDA in line with the British Columbia and Alberta privacy statutes. The exception allows parties to a prospective business transaction to use and disclose an individual's personal information without his or her knowledge or consent if the information is necessary to determine whether to proceed with the transaction and to complete it. An organization that provides personal information must have an agreement that requires it (i) to use and disclose the information only for purposes relating to the transaction, and (ii) to protect the information and return or destroy it if the transaction does not proceed.

Once the business transaction is complete, the organization receiving the personal information may use and disclose that information before or during the transaction without the individual's knowledge and consent if

- the agreement between the organizations requires them to use and disclose the personal information for the purposes for which it was used or disclosed during the transaction, to protect the information appropriately and to give effect to withdrawals of consent;
- the personal information is necessary for carrying on the business that was the object of the transaction; and
- one of the parties notifies the individual within a reasonable time that the information was disclosed before or during the transaction.

Data-Breach Notification Requirements

The Act now contains mandatory data-breach notification requirements in cases in which it is reasonable for an organization to believe that a breach of its security safeguards creates "a real risk of significant harm to an individual". This assessment is based on the sensitivity of the personal information; the probability that the personal information has been, is being or will be misused; and any other prescribed factor. "Significant harm" is defined broadly and includes bodily harm; humiliation; damage to reputation or relationships; loss of

employment, business or professional opportunities; financial loss; identity theft; negative effects on a credit record; and damage to or loss of property. In these cases, an organization must do the following:

- Report the breach to the Commissioner as soon as feasible.
- Notify the individual unless prohibited by law from doing so. The notification must be conspicuous, must be given directly to the individual if feasible, must be given as soon as feasible and must allow the individual to understand the significance of the breach and take whatever steps possible to reduce the risk.
- Notify other organizations, including government institutions, as soon as feasible, if the notifying organization believes that the other organization or government institution can mitigate the risk resulting from the breach.

Organizations in control of personal information must now keep and maintain records of every breach of security safeguards involving personal information.

Fines for failure to comply with the data-breach rules can be as high as $100,000 under the new amendments. As noted above, the current voluntary notification regime remains in effect until regulations are passed.

Consent Requirements

The Act has also been clarified to confirm that consent is only considered valid if it is reasonable for the organization using, collecting and disclosing personal information to expect that the individual would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which he or she is consenting.

Collection, Use and Disclosure of Personal Information Without the Individual's Consent

The amendments include an extension of the rules regarding the collection, use and disclosure of personal information without the individual's knowledge or consent.

Organizations may collect, use or disclose personal information without knowledge or consent if it is contained in a witness statement and the collection is necessary to assess, process or settle an insurance claim or if that information was produced by the individual in the course of employment or business or professional services and the collection is consistent with the purpose for which the information was produced.

Disclosure is also allowed without the individual's knowledge or consent if disclosure is made to identify an ill, injured or deceased individual or to communicate with the person's next of kin; to prevent or investigate financial abuse; or for the purposes of detecting or preventing fraud, if such knowledge or consent would compromise the investigation or ability to prevent, detect or suppress the fraud.

In addition, a federal work, undertaking or business may collect, use and disclose personal information without an individual's consent if doing so is necessary to establish, manage or terminate an employment relationship with that individual and that individual has been informed that the information will or may be collected, used or disclosed for those purposes.

Key Contact: Elliot A. Greenstone