[redacted] June 24, 2015 10:20 AM

[redacted] FYI: Canada's Digital Privacy Act Amends PIPEDA

Digital Privacy Act Modernizes PIPEDA

http://www.jdsupra.com/legalnews/digital-privacy-act-modernizes-pipeda-20301/

6/23/2015

By

Stephen D. Burns,
J. Sébastien A. Gittens
Graeme Harrison
Martin P.J. Kratz Q.C.
Michael Whitt Q.C.
Bennett Jones LLP

On June 18, 2015, significant portions of the Digital Privacy Act received Royal Assent. This Act, amends the Personal Information Protection and Electronic Documents Act (PIPEDA), and brings important certainty to how organizations can collect, use and disclose personal information in the course of business and otherwise modernizes PIPEDA based on other Canadian experience with privacy law over the past decade or more.

Business Transactions Exemption

Organizations subject to PIPEDA finally have certainty on what is expected of them in the context of a business transaction. PIPEDA's new provisions when structuring commercial transactions are akin to the "business transaction" exemptions under Alberta and British Columbia's Personal Information and Protection Act (PIPA). Section 7 of PIPEDA sets out a regime for the use and disclosure of personal information, without knowledge or consent, by parties to a prospective "business transaction". Under PIPEDA, "business transactions" includes purchase and sale transactions, mergers and amalgamations, and the extension of loans or other financing, and other commercial arrangements.

PIPEDA provides that this exemption only applies to personal information that is "necessary" for determining whether to proceed with or complete a transaction, and requires that the organizations have entered into an agreement requiring the organization that receives such personal information to: (i) use and disclose that information solely for purposes related to the transaction; (ii) protect that information by security safeguards appropriate to the sensitivity of the information. The organization that receives the personal information must also return or destroy the information if the transaction does not proceed.

Reflecting the requirements in British Columbia's PIPA, the exemption requires that, in the case of a completed transaction, at least one of the parties must notify the individuals whose information has been disclosed that the transaction is complete and that the information has been so disclosed.

Notably, the provisions of section 7 do not apply where the "primary purpose or result" of the business transaction is the purchase, sale, acquisition or disposition of personal information itself.

New Data Breach Notification Obligations

Organizations subject to PIPEDA should also be aware of the upcoming obligations that PIPEDA will place on them with respect to breaches of their security safeguards. This aspect of the law will come into force once regulations have been finalized. Once the applicable provisions are proclaimed, PIPEDA will define "breach of security safeguards" as a loss or unauthorized access or disclosure of personal information that results from either the breach of an organization's security safeguards, or an organizations failure to establish these safeguards in the first place.

PIPEDA will require that organizations report to both the Commissioner and the individual in question where it is reasonable in the circumstances to believe that the breach creates a "real risk of significant harm" to an individual. PIPEDA sets out the factors relevant to consider in determining whether there is a "real risk of significant harm", and what constitutes "significant harm" include the sensitivity of the personal information involved in the breach, the probability that the personal information has been, is being or will be misused and other factors identified by regulation. The Act also provides that the notification shall be given as soon as feasible after the organization determines that the breach has occurred.

The affected organization also will have an obligation to notify other organizations and governmental institutions if such other organizations or institutions may be able to reduce or mitigate the risk of harm.

Organizations should be aware that these and other obligations are backed up by new compliance and enforcement measures. PIPEDA will make it an offence to knowingly contravene the obligation to report to the Commissioner. The Commissioner will also be empowered to enter into

“compliance agreements” with organizations, and to apply to the Court for an order directing an organization to comply.

Alberta PIPA has had mandatory breach reporting in place since 2010 for cases where there “exists a real risk of significant harm to an individual” as a result of the loss or unauthorized access or disclosure. As a result organizations who seek to anticipate the impact of the changes may study the Alberta experience.

Other Amendments

In addition to the amendments discussed above, PIPEDA now includes protections for the personal information of federally regulated job applicants.

Additional exemptions to consent have also been enacted, which permits an organization to use personal information without consent in certain circumstances, including the prevention of fraud.

A limitation on consent has also been added in a new Section 6.1. The new provision states that “the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.” It is presently unclear how this limitation will be interpreted by the Courts and the Commissioner’s office. As a result organizations should review the clarity and completeness of their privacy policies and privacy disclosures.

Finally, whistleblower protections have also been included within the scope of the new amendments.

Together, the provisions of the Digital Privacy Act will modernize how organizations subject to PIPEDA deal with the personal information of individuals.

D. Reed Freeman | WilmerHale
[redacted]

Follow our Cybersecurity, Privacy and Communications Group on Twitter @WHCyberPrivacy

Please consider the environment before printing this email.