LAPOINTE ROSENSTEIN MARCHAND MELANÇON
L.L.P. Attorneys

Newsletter

Commercial Law

December 2015

M^tre Marissa Carnevale

This newsletter was written in collaboration with Mr. Vinay Desai, articling student, and Ms. Aude Florin, student.

Important Amendments to Canada's Privacy Laws

On June 18, 2015, Canada's *Digital Privacy Act* (the "**DPA**") received royal assent and became law. The DPA amends the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), Canada's private sector data protection statute. Many of the important amendments are discussed below.

The DPA has already come into effect, except for the breach reporting provisions discussed in Section 1 below, which will come into effect at a date still to be determined.

1. Breach Reporting (Not Yet in Force)

Once the breach reporting provisions of PIPEDA come into force, organizations that suffer a data security breach will be required to report the breach to affected individuals and to the Privacy Commissioner of Canada if, in the circumstances, "it is reasonable to believe that" the breach creates a "real risk of significant harm to [the] individual".

A security breach is defined as any (i) loss or (ii) unauthorized access or (iii) disclosure of personal information due to a breach of an organization's security safeguards or failure to initially establish same. The definition of "significant harm" is open-ended and "includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property". The determination of whether a security breach poses a "real risk" is based on the factors set out in PIPEDA, namely, the sensitivity of the information in question and the likelihood that it is being misused or may be misused.

Government institutions and other organizations will also need to be notified in certain circumstances if they can reduce or mitigate the risk of the harm that could result from the breach.

The collective effect of these legislative amendments, which represent significant changes as compared to Canada's current privacy legislation, is increased awareness and broadened protections for individuals whose personal information is subject to a data security breach.

It is also important to note that organizations will be required to keep records of *all* data breaches, including those that do not give rise to mandatory reporting. These records must be made available to the Privacy Commissioner on request. Organizations that knowingly fail to report or record a breach may be guilty of an offence punishable by a fine of up to $100,000.

2. Business Transaction Exemption

PIPEDA now contains a "business transaction" exemption allowing organizations to use and disclose personal information without the consent of an individual in the context of a broad range of prospective transactions including purchase and sale transactions, mergers and acquisitions, financing, leasing and other commercial arrangements. This new exemption is meant to facilitate business transactions as it permits the disclosure of information during a due diligence process and as part of a transition.

Certain restrictions apply, however: the transfer of personal information must not be the primary purpose of

the transaction and the information must be necessary for the completion of the transaction. These restrictions seem appropriate given the overall objectives of PIPEDA and the risks it strives to address.

The law provides an additional layer of protection for personal information disclosed under the "business transaction" exemption: the organization that receives the personal information must only use it for purposes related to the transaction, and must safeguard the information and return or destroy it if the transaction is not completed. If a transaction is in fact completed, additional requirements apply to the continued use of the personal information exchanged without the knowledge or consent of the individuals concerned.

3. Informed Consent

PIPEDA now provides further clarification on the requirements applicable to obtaining an individual's consent for purposes of collecting, using and disclosing their personal information. An individual's consent is only valid "if it is reasonable to expect" that the individual "would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting".

This new limitation will require organizations to clearly explain the nature of their use of an individual's personal information in a manner that they will understand.

4. Business Contact Information

PIPEDA previously provided that an individual's business contact details did not constitute personal information; this information was therefore outside the scope of PIPEDA's protections. Further to the amendments under the DPA, PIPEDA introduces a new definition for "business contact information", which includes a person's position, name or title, work address, work telephone number, work fax number or work e-mail address. The definition of "personal information" in PIPEDA now refers simply to "information about an identifiable individual", which would include "business contact information".

PIPEDA's provisions requiring consent for the collection, use and disclosure of personal information do not apply to business contact information where such information is collected, used or disclosed for the purpose of communicating with the individual in relation to their business, position or employment.

As a result, PIPEDA's protections would now generally apply to business contact information unless it is used in the context of an individual's business or employment dealings.

It should be noted that Quebec's private sector privacy legislation does not contain a similar exception for business contact information, which would generally be considered information about an identifiable individual and would be subject to the protections established pursuant to such legislation regardless of the context in which it is used.

5. Disclosure Without Consent for Enforcement

New PIPEDA provisions will, in certain cases, allow an organization to disclose personal information in certain cases without the knowledge or consent of the individual in question. For example, personal information may be disclosed without consent in order to investigate a violation or anticipated violation of a provincial or federal law or for the purposes of detecting or preventing fraud, whenever it is reasonable to believe that obtaining consent would compromise the outcome of such an investigation or endeavour.

It is important to note that these provisions do not require organizations to share information in the circumstances described, but merely allow the possibility of disclosure for the prescribed purposes.

6. Public Announcements

The DPA also amends PIPEDA by expressly allowing the Privacy Commissioner to make public any information it obtains if it believes it is in the public interest. Coupled with the new requirements for mandatory breach reporting and record-keeping, these legislative amendments provide significant discretion to the Privacy Commissioner with respect to the possibility of making disclosures with respect to privacy breaches suffered by organizations.

Suggested Tips for Your Business

The DPA's amendments to PIPEDA generally include broader powers for the Privacy Commissioner of Canada, as well as enhanced penalties for violations. As data privacy and security becomes increasingly regulated, and organizations' customers and employees become increasingly vulnerable to the effects of data security breaches, organizations must strive to put adequate safeguards in place and continuously monitor their systems and networks for potential weaknesses. They should also carefully review their privacy policies and practices in order to ensure that consent is being validly obtained and that individuals are not being misled with respect to the use that is made of their personal information.

Organizations must also prepare for breach record-keeping and reporting requirements and should strive towards putting adequate security breach contingency plans in place, which may include sensitizing employees, training public relations staff and obtaining data security insurance coverage where applicable.

For more information, please contact:

Marissa Carnevale
514 925-6324
marissa.carnevale@lrmm.com