LAPOINTE ROSENSTEIN MARCHAND MELANÇON
L.L.P. Attorneys

Local Counsel Canada & Quebec

Last updated: November 2015

Marissa Carnevale, Attorney

Essentials of Privacy Law

Privacy laws have been adopted in jurisdictions worldwide to curtail the effects of invasive and careless methods that businesses use to share personal information, including demographic data, preferences, habits and other similar information.

CANADA

The *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), Canada's private sector data protection statute, contains significant protections for individuals whose personal information may be collected, used and shared by people or entities with which they have dealings.

Informed Consent

In general, a person must consent to any use of their personal information. Under PIPEDA, 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 requires organizations to clearly explain the nature of their use of an individual's personal information in a manner that they will understand.

In order to collect, convey or make use of personal information, the projected uses of information about an identifiable individual must be disclosed. In other words, where the purposes for collecting, using, storing and disclosing an individual's personal information are not clearly explained, the individual will likely not have provided valid consent to use the personal information. In particular, if they unknowingly or unwittingly agree for their personal information to be processed and shared by a business that collects, uses or discloses it for any unexpected or unreasonable purpose, their consent will likely not be valid for such purposes.

In Canada, the law also requires disclosure where data may be processed or stored in other countries or by entities other than the one collecting the data, whether domestically or abroad, even if such processing or storage is done on behalf of the entity collecting the data.

Business Transaction Exemption

PIPEDA 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 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.

PIPEDA 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.

Business Contact Information

PIPEDA's provisions requiring consent for the collection, use and disclosure of personal information do not apply to business contact information (such as a person's position, name or title, work address, work telephone number, work fax number or work email address) 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 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 (discussed in additional detail below) does not contain a similar exception for business contact information, which would be considered information about an identifiable individual and would generally be subject to the protections established pursuant to such legislation regardless of the context in which it is used.

Public Announcements

PIPEDA expressly allows Canada's Privacy Commissioner to make public any information it obtains if it believes it is in the public interest.

QUEBEC

The *Act respecting the protection of personal information in the private sector* (the "**Quebec Privacy Act**") imposes similar restrictions on those doing business in Quebec who collect, store and process personal information about individuals, including employees and customers.

In addition, the Quebec Privacy Act requires an organization doing business in Quebec who entrusts a person outside Quebec with "holding, using or communicating such information on its behalf to take "all reasonable steps to ensure" that the information will be used only for the purposes for which consent was obtained and will not be "communicated to third parties" without such consent. Moreover, if an organization doing business in Quebec considers that the information "will not receive the protection" required under the Quebec Privacy Act, the organization "*must* refuse to communicate the information or refuse to entrust a person or a body outside Quebec with the task of holding, using or communicating it" on its behalf.

RECENT AMENDMENTS

Breach Reporting (Not Yet in Force)

On June 18, 2015, Canada's *Digital Privacy Act*, (the "**DPA**") received royal assent and became law. The DPA contains provisions regarding mandatory breach reporting, which will come into effect at a date still to be determined and will constitute significant amendments to PIPEDA and its enforcement.

Once mandatory breach reporting comes 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 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 harm that could result from the breach.

The collective effect of these legislative amendments 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 up to $100,000.

Coupled with the Privacy Commissioner's right to make public announcements with respect to privacy concerns that rise to the level of public interest, mandatory breach reporting and record-keeping will confer significant discretion upon the Privacy Commissioner with respect to the possibility of making disclosures in connection with privacy breaches suffered by organizations.

For more information, please contact:

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