FTR Now

New Privacy Legislation in Manitoba

Date: September 30, 2013

Organizations with operations in Manitoba need to be aware that the Manitoba Legislature has recently passed new privacy legislation that will apply to the private sector and, to a lesser degree, to the not-for-profit sector – The Personal Information Protection and Identity Theft Prevention Act ("PIPITPA" or the "Act"). PIPITPA will establish rules for the collection, use and disclosure of personal information, including employee information, for most organizations in the province.

In this *FTR Now*, we will provide a brief overview of the new legislation and how it will affect organizations in Manitoba.

BACKGROUND

PIPITPA is the result of a Private Member's Bill, Bill 211, which was introduced by a member of the Progressive Conservative opposition party. The Bill was passed by a unanimous Legislature on September 12, 2013, and was given Royal Assent on September 13th. The new Act is not in force yet, but is awaiting proclamation.

PIPITPA is the first private sector privacy legislation to be passed in Canada since the British Columbia and Alberta statutes came into effect in January of 2004. Indeed, the Act shares many similarities with the B.C. and Alberta Acts. The following discussion highlights some of the key elements of the legislation. At this time, the federal government has not determined whether PIPITPA is "substantially similar" legislation, such that it will replace the *Personal Information Protection and Electronic Documents Act* within the province. However, it can be anticipated that such a declaration would issue in due course.

SCOPE OF APPLICATION

Subject to some limited exceptions, PIPITPA will apply to every organization that operates in Manitoba and that collects, uses and discloses personal information (including personal employee information). One key exception applies to "public bodies" that are governed by *The Freedom of Information and Protection of Privacy Act*.

Two other categories of organizations – professional regulatory organizations and non-profit organizations – are carved out of the main provisions of the Act. For professional regulatory organizations, the Act allows for regulations to be made under which the organizations may

establish “personal information codes” that would apply in place of the Act. For non-profit organizations (to be defined by regulation), the Act would only apply to the collection, use and disclosure of personal information in the course of commercial activities, but would otherwise not apply generally to these organizations.

The Act will not apply to the collection, use and disclosure of personal information in a number of situations, including if these activities are done solely for personal or domestic, artistic or literary, or journalistic purposes. Similarly, the Act would not apply to the collection, use or disclosure of business contact information provided that the individual was being contacted in his or her capacity of employee or official in an organization.

GENERAL OBLIGATIONS

Organizations subject to the Act are responsible for the personal information that is in their custody or under their control. There is an obligation to appoint an individual who is responsible for compliance with the Act, and to ensure compliance by any person who handles personal information on the organization’s behalf.

Organizations are also required to establish policies and practices that will ensure reasonable compliance with the Act. Upon request, an organization will be required to provide information about its policies and practices.

The Act generally operates as a consent-based model – namely, the general rule is that organizations will require an individual’s consent to collect, use or disclose the individual’s personal information. Collection of personal information should generally be from the individual in question. Individuals are given the ability to provide limited consents, or to withdraw or limit consents already given.

The Act also allows for the use of “opt out” consents, though this appears to be limited to less sensitive personal information. Similarly, in certain circumstances in which individuals volunteer their personal information for a particular purpose, they will be deemed to have consented to its collection, use and disclosure for that purpose.

COLLECTION, USE AND DISCLOSURE

PIPITPA establishes a reasonableness threshold for the collection of personal information. An organization may collect personal information only for reasonable purposes, and may only collect information that is reasonable for meeting those purposes. As a general rule, before collecting personal information an organization must notify the individual of the purposes for the collection, as well as the name of a person who can answer questions on behalf of the organization.

As noted earlier, PIPITPA also establishes a general requirement that the collection, use and

disclosure of personal information requires an individual's consent. Nevertheless, as is common in personal information protection statutes, the Act also contains a number of exceptions to the general consent requirement. For example, consent is not needed if a collection, use or disclosure is required by law, is part of an investigation or legal proceeding or is publicly available. Readers should consult the statute for the full range of exceptions.

Importantly, PIPITPA contains special rules that apply to "personal employee information", which is information about an employee or potential employee that is reasonably required by an organization for the purposes of establishing, managing or terminating an employment relationship or a volunteer work relationship. The Act defines "employee" very broadly to include apprentices, volunteers, students and agency employees.

For "personal employee information", PIPITPA carves out exceptions to the consent rule if the collection, use or disclosure of personal information is about an employee of an organization or is used to recruit potential employees. In those cases, consent is not required provided that the collection, use or disclosure is reasonable for its purposes, the information relates solely to the employment relationship, and for current employees, notice is provided of the collection, use or disclosure and the underlying purposes. [We note that the consent exception is extended to former employees with respect to the disclosure of personal information only, but not to its collection or use.]

BUSINESS TRANSACTIONS

PIPITPA contains provisions relating to business transactions and proposed business transactions to enable the transfer of personal information without consent in order to facilitate the transaction. The Act specifies numerous requirements including the need for written agreements relating to the information, and obligations to return or destroy personal information should the business transaction not proceed. Notably, these provisions do not apply if the primary purpose of the transaction is the purchase, sale, lease, etc., of personal information itself.

BREACH NOTIFICATION AND A RIGHT OF ACTION

PIPITPA contains a broadly worded breach notification obligation, subject to two important qualifications. As a general rule, an organization must notify affected individuals if personal information in its custody or under its control is "stolen, lost or accessed in an unauthorized manner". This must typically be done as soon as reasonably practicable, and following any process specified in the regulations.

The breach notification obligation does not apply, however, if:

- a law enforcement agency is investigating the breach and instructs the organization not to disclose the breach; or

- the organization is “satisfied that it is not reasonably possible for the personal information to be used unlawfully”.

The second exception is an important one, and gives organizations the opportunity to assess risk of unlawful use before determining whether a breach notification is required. This is the second private sector privacy statute in Canada to feature a breach notification rule. Alberta’s rule is arguably broader because it requires notification based on the potential for “harm” and not merely unlawful use.

PIPITPA provides individuals with a statutory right of action for failures to protect personal information and for failures to notify as required by the Act. The statutory action allows individuals to claim “damages arising” out of the respective failures. The Act does not expressly define damages to encompass “moral” damages or damages for non-pecuniary loss.

ACCESS AND CORRECTION RIGHTS

Like most privacy legislation, PIPITPA also contains broad rights of access and correction. The Act establishes a detailed access and correction process, and permits organizations to refuse access in limited circumstances. Reasonable fees may be charged for access, and the Act contemplates that regulations may be passed to deal with fee-related issues.

Rights of correction are also not absolute, and organizations may refuse to correct information if they are satisfied on reasonable grounds that a correction should not be made. However, the record containing the personal information must be annotated with the correction that was requested and not made.

CONCLUSION

Interestingly, unlike Manitoba’s public sector statute, PIPITPA does not currently include an enforcement mechanism by which individuals may file complaints with the office of the Ombudsman (though, curiously, the whistle-blower protection in the Act contemplates that employees might approach with Ombudsman with allegations of non-compliance). This would appear to be a key omission from the legislation, and leaves open the significant question as to how the Act will be enforced in practice. We will continue to monitor developments to see if this omission is addressed before the Act is proclaimed in force.

The passage of PIPITPA is an important development in the ongoing evolution of privacy law in Canada. For organizations that operate in Manitoba, the Act will have a direct impact on your practices surrounding the collection, use and disclosure of personal information, and the security practices you employ for this information.

For other organizations, the passage of this new statute raises the possibility that other provinces

will follow suit and introduce similar legislation. At present, a majority of provinces, including Ontario, continue to operate without their own privacy legislation for the private sector, leaving the field to be partially regulated by PIPEDA and the common law.

We will continue to monitor and report on privacy-related developments throughout Canada as they may apply to employers and other organizations. If you have any questions about the new Manitoba statute or any other privacy-related matter, please contact any member of our Information Management & Privacy Practice Group.
