0: PRIVACY LAW

THE ROCKIES

Canada's most visited mountain range, the Rockies, is an international destination for sports, sightseeing and escape from the daily grind.

Privacy is important to Canadians. With advances in technology, organizations are collecting, storing, transferring and disclosing more personal information about their consumers and employees than ever before. The accumulation of personal information increases the risks for organizations doing business in Canada.

In an age of social media, cloud computing, global networks and international data flows, incidents involving data security breaches and identity theft frequently make headlines in Canada — particularly given the advent of class action law suits to remedy privacy breaches. As a result, privacy protection is an increasingly pressing public-policy concern.

Canada has enacted comprehensive federal privacy legislation that applies to the private sector. In addition, certain provinces have enacted both comprehensive and industry-specific private sector privacy legislation.

1. THE PRIVACY LANDSCAPE IN CANADA

a. Federal

In Canada, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) regulates the collection, use and disclosure of personal information in the private sector. "Personal information" is broadly defined in the Act as any "information about an identifiable individual" whether public or private, with limited exceptions.

PIPEDA applies to federal works, undertakings and businesses, and to private sector organizations that collect, use or disclose personal information in the course of commercial activities in provinces that do not have substantially similar legislation. PIPEDA's application to personal employee information is limited to organizations that are federal works, undertakings and businesses.

EXAMPLES OF THESE ORGANIZATIONS INCLUDE:

- Airlines
- Banks
- Broadcasting
- Interprovincial railways
- Interprovincial or international trucking, shipping or other forms of transportation
- Nuclear energy
- Activities related to maritime navigation

PIPEDA is a general law that applies to the collection of personal information regardless of the technology used, and applies to all personal information that flows across provincial or national borders in the course of commercial transactions.

Compliance with PIPEDA is subject to an overriding standard of reasonableness whereby organizations may only collect, use and disclose personal information for purposes that a "reasonable person would consider appropriate in the circumstances." This requirement applies even if the individual has consented to the collection, use or disclosure of their personal information.

In provinces with privacy legislation that the federal government has deemed to be "substantially similar" to PIPEDA, the Act does not apply. Currently, only Alberta, British Columbia and Québec have "substantially similar" privacy legislation in place. However, PIPEDA continues to apply to federal works, undertakings or businesses that operate in those provinces.

In addition, health information custodians — such as physicians, nurses and hospitals — in Ontario, Newfoundland and Labrador, and New Brunswick are exempt from PIPEDA with respect to personal health information, as these provinces have specific health information privacy statutes that have been deemed "substantially similar" to PIPEDA. Organizations that operate interprovincially or internationally are required to deal with both provincial and federal privacy legislation.

The *Digital Privacy Act* was passed by Parliament and received royal assent in June 2015. The Act makes several important amendments to PIPEDA, including new mandatory breach reporting requirements for organizations and enhanced enforcement powers for the privacy commissioner of Canada. It is important to note that some of the amendments have not yet come into force.

b. Provincial

Alberta, B.C. and Québec have also enacted comprehensive private sector privacy legislation, entitled the *Personal Information Protection Act* (PIPA) in Alberta and B.C., and *An Act respecting the protection of personal information in the private sector* (*Québec Privacy Act*) in Québec.

While these provincial laws are similar in principle to PIPEDA, there are important differences in the details. These laws apply generally to all private sector organizations with respect to the collection, use and disclosure of personal information — not just with respect to commercial activities — and to the personal information of employees. The *Québec Privacy Act* also applies to private sector collection, use and disclosure of personal health information.

C. LEGISLATIVE OVERVIEW

All Canadian privacy legislation, including PIPEDA, reflects the following 10 principles set out in the Organisation for Economic Co-operation and Development Guidelines, created in the early 1980s:

- Accountability
- Identifying purposes
- Consent
- Limiting collection
- Limiting use, disclosure and retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance

As outlined in the "federal" section above, the standard of reasonableness is considered the overarching rule in Canadian privacy legislation. One cannot avoid this standard by obtaining consent to an objectively unreasonable collection, use or disclosure of their information. In most cases, organizations must have either the express or implied consent of the individual to the collection, use or disclosure of their personal information. All four principal private sector statutes apply similar principles:

- Personal information may only be collected, used or disclosed with the knowledge and consent of the individual.
- The collection of personal information must be limited to what is necessary for identified purposes.
- Personal information must be collected by fair and lawful means.

Personal information must be protected by safeguards appropriate for the level of sensitivity of the information. For example, highly sensitive information, such as financial data, must be provided with a proportionately high level of security that should include physical, organizational and technological protection measures. As well, individuals must be provided with easy access to information about an organization's privacy policies and practices.

Alberta, B.C. (with regard to certain designated databases), Manitoba, Ontario, Saskatchewan, New Brunswick, Nova Scotia, and Newfoundland and Labrador have legislation specifically governing the collection and use of personal health information. Prince Edward Island, the Northwest Territories and the Yukon have recently introduced new legislation aimed at protecting personal health information, which is expected to come into force in late 2015. Currently, the management and sharing of personal health information in all of these provinces and territories is governed by the general public and private sector privacy legislation. All Canadian provinces and territories have enacted legislation that regulates the collection, use and disclosure of personal information in the public sector.

In specific industry sectors, additional requirements will apply depending on the nature of the consent sought. For example, several provinces, including Ontario and Nova Scotia, impose font size requirements on requests for consent/notice prior to obtaining a credit bureau report.

2. EMPLOYERS

In accordance with constitutional limits placed on federal legislation, PIPEDA applies only to the employment information of employees of federally regulated organizations, such as banks, airlines and telecommunications companies. Provincial privacy legislation applies to employee information outside of those sectors. Unlike PIPEDA, the *Québec Private Sector Act* does not expressly exclude from the scope of its definition information relating to "professional/employment status" — such as an individual's name, title or business address, or telephone number at work.

Under the Alberta PIPA and the B.C. PIPA, employers are permitted to collect, use or disclose "personal employee information" without the consent of the employee if it is reasonably required for the purposes of establishing, managing or terminating an employment relationship. PIPEDA does not have a similar provision dealing with the collection, use and disclosure of personal information in the workplace.

However, PIPEDA permits reliance on implied consent if the collection, use or disclosure of the information is for purposes that a reasonable person would consider appropriate in the circumstances. Again, the concept of reasonableness is central to whether an employer is required to obtain explicit consent.

3. REPORTING PRIVACY BREACHES

Unlike the U.S., where the majority of states have enacted mandatory data breach notification rules, Canada currently has limited requirements for organizations to proactively notify individuals or the appropriate regulatory bodies of a data breach. The exceptions are *Ontario's Personal Health Information Protection Act*, Newfoundland and Labrador's *Personal Health Information Act*, New Brunswick's *Personal Health Information Privacy and Access Act*, and Alberta's PIPA, all of which require mandatory data breach notification. However, the exception is likely to become the rule in the foreseeable future. Section 10 of the recently enacted *Digital Privacy Act* adds a new provision to PIPEDA, which will require mandatory breach notification as soon as this section comes into force.

Alberta was the first Canadian jurisdiction to require mandatory privacy-breach notification in the private (non health-related) sector. Organizations subject to Alberta's PIPA are required to notify the province's information and privacy commissioner if personal information under the organization's control is lost, accessed or disclosed without authorization, or if it has in any way suffered a privacy breach, where a real risk of significant harm to an individual exists as a result of the breach. In those circumstances, failure to notify the commissioner of a breach is an offence.

The notification requirement is only triggered if the harm threshold is met, which is defined as "where a reasonable person would consider that there exists a real risk of significant harm to an individual." The commissioner has interpreted "significant harm" to mean "a material harm… [having] non-trivial consequences or effects." Examples may include possible financial loss, identity theft, physical harm, humiliation or damage to one's professional or personal reputation.

Furthermore, the commissioner requires that a "real risk of significant harm" must be more than "merely speculative" and not simply "hypothetical or theoretical." A breach relating to highly sensitive personal information, such as financial information, is more likely to meet this standard and require reporting.

If a breach meets the threshold of being a "real risk of significant harm" and is reported appropriately, the commissioner will review the information provided by the organization to determine whether affected individuals need to be notified of the data breach. If so, the commissioner can direct the organization to notify individuals in the form and manner prescribed by PIPA regulations.

Once section 10 of the *Digital Privacy Act* amending PIPEDA comes into force, organizations that suffer a data breach that creates a "real risk of significant harm" to one or more individuals will be required to take the following measures, as soon as feasible:

i. Report the incident to the commissioner.

ii. Notify all individuals affected by the breach, and inform them of any steps they can take to minimize harm. Make sure that sufficient detail is provided to the affected individuals to enable them to understand the significance of the breach.

iii. Where the organization has notified affected individuals, it must also notify any other organizations or government entities of the breach if it believes that such action may reduce the risk of harm.

iv. Maintain a record of every security data breach and make such records are available to the commissioner on request.

The *Digital Privacy Act* defines "significant harm" broadly to include "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identify theft, negative effects on the credit record and damages to or loss of property." The Act determines the existence of a "real risk of significant harm" by reference to the sensitivity of the personal information involved in the breach, the probability that the personal information will be misused, and any other factors that may be prescribed by regulation.

As well, the Act will amend PIPEDA to create offences for non-compliance with data security breach obligations. After this section comes into force, an organization that fails to report and record a breach —or that hinders the commissioner's efforts to investigate a complaint or perform an audit — may face fines of up to $10,000 for a summary offence, or up to $100,000 for an indictable offence.

4. CROSS-BORDER TRANSFERS AND OUTSOURCING

Cross-border transfers and the outsourcing of Canadian personal information to foreign countries have become subjects of much focus in Canada. A great deal of this attention has centred on concerns that U.S. authorities could use the *USA Patriot Act* to obtain Canadians' personal information if it is located in or accessible from the U.S.

PIPEDA and related provincial legislation do not prohibit the transfer of personal information outside of Canada. However, public sector privacy legislation in B.C. and Nova Scotia imposes restrictions on public bodies (and organizations that process personal information on their behalf) with respect to the transfer of personal information. Furthermore, privacy regulators have generally held that notice of such transfers should beprovided to affected individuals — along with notice that such personal information may be subject to access requests from foreign governments, courts, law enforcement officials and national security authorities according to foreign laws.

PIPEDA requires an organization to provide a "comparable level of protection" when personal information is being processed by a third party through "contractual or other means." As such, if an organization transfers personal information to a third party, the transfer must be "reasonable" for the purposes for which the information was initially collected, the information must be protected using contractual means, and the organization should be transparent about its information-handling practices, including notifying individuals. In addition, the *Québec Privacy Act* requires organizations to consider the potential risks involved in transferring personal information outside of Québec. If the information will not receive adequate protection, it should not be transferred.

The Alberta PIPA explicitly imposes obligations on organizations that use service providers outside of Canada to collect, use, disclose or store personal information. Organizations are obligated to notify individuals that they will be transferring individuals' personal information to a service provider outside of Canada, and to include information on outsourcing practices in the organization's policies.

5. ENFORCEMENT

In addition to negative publicity, there are legal and financial consequences for violating privacy legislation. An injured party, be it an individual or organization, must follow the ombudsman's procedure of filing a complaint with the respective provincial authority or the federal Office of the Privacy Commissioner (OPC).

The role of the OPC is to facilitate the resolution of such complaints through persuasion, negotiation and mediation. The OPC may decide to investigate the complaint and to issue a report setting out non-binding recommendations based on the findings. In conducting the investigation, the OPC has a variety of powers, including the power to compel the production of evidence.

Once the OPC completes its investigation and issues a report, either the OPC or the complainant may apply to the Federal Court to seek enforcement and/or damages under PIPEDA. The OPC can also impose a fine for noncompliance with certain provisions of PIPEDA.

Under the Alberta PIPA and B.C.'s PIPA, the applicable provincial privacy commissioner has the power, following an investigation, to direct the organization to remedy the situation. These orders are enforceable in court and are the basis for civil actions. In Québec, orders of that province's privacy commission (Commission d'accès à l'information) can be appealed to the Québec Superior Court.

With the amendment to PIPEDA by section 15 of the *Digital Privacy Act* now in force, the commissioner can enter into compliance agreements with organizations that he or she reasonably believes have violated, or are about to violate, PIPEDA provisions. Such agreements can include any terms the commissioner considers necessary to ensure compliance with PIPEDA. If a counterparty organization breaches the agreement, the commissioner is authorized to apply to the Federal Court for a compliance order or a hearing. However, being party to a compliance agreement will not insulate the organization from claims made by individuals or from the prosecution of an offence under PIPEDA.

Learn more about Gowling WLG services in this area at gowlingwlg.com/privacy-canada