

O

Privacy Law



Privacy and the protection of personal information are important to Canadians. With advances in technology, organizations are collecting, storing, transferring and disclosing more personal information about their consumers and employees than they have in the past. The accumulation of personal information increases the risks for organizations that do business in Canada. This is an age of social media,

cloud computing, global computer networks and international data flows. Breaches of data security and cases of identity theft frequently make headlines in Canada, and 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 PIPEDA and includes 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. Examples of federal works and undertakings in Canada include airlines, banks, broadcasting, interprovincial railways, interprovincial or international trucking, shipping or other forms of transportation, nuclear energy and activities related to maritime navigation.

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

Compliance with PIPEDA is subject to an overriding standard of reasonableness whereby organizations may only collect, use and disclose personal information for the 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.

PIPEDA does not apply in provinces with privacy legislation that is substantially similar to it. Currently, only Alberta, British Columbia and Québec have legislation that has been declared substantially similar to PIPEDA. It should be noted, however, that PIPEDA does apply to federal works, undertakings or businesses that operate in those provinces. In addition, Ontario health information custodians (such as physicians, nurses and hospitals) have been exempted from PIPEDA with respect to personal health information, as Ontario has a specific health-information privacy statute that applies. Organizations that operate interprovincially are required to deal with both provincial and federal privacy legislation.

b. Provincial

Alberta and British Columbia have also enacted comprehensive private-sector privacy legislation, entitled the *Personal Information Protection Act* (PIPA) in both provinces, which applies generally and includes the personal information of employees.

Québec’s private-sector privacy legislation, *An Act respecting the protection of personal information in the private sector* (*Québec Privacy Act*), is similar in principle to PIPEDA; however, there are important differences

in detail. The *Québec Privacy Act* applies to all private-sector organizations with respect to collection, use and disclosure of personal information (not just with respect to commercial activities) and to employee information. It also applies to private-sector collection, use and disclosure of personal health information.

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

The overarching rule in Canadian privacy legislation is that organizations may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. This rule applies regardless of the consent of the individual whose information is in question. One cannot avoid the reasonableness standard by obtaining consent to an objectively unreasonable collection, use or disclosure of their information. All four principle 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; and
- Personal information must be collected by fair and lawful means.

Additionally, personal information must be protected by adequate safeguards, and individuals must be provided with easy access to information about an organization's privacy policies and practices.

Alberta, Manitoba, Ontario, Saskatchewan, New Brunswick and Newfoundland and Labrador have legislation specifically governing the collection and use of personal health information, and all provinces in Canada have enacted legislation that regulates the collection, use and disclosure of personal information in the public sector.

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 those sectors.

Under the Alberta PIPA and the British Columbia 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 states that there is implied consent if the collection, use or disclosure was 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 United States, 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 in such circumstances. 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.

Alberta is the first Canadian jurisdiction to require mandatory privacy-breach notification in the private sector. Organizations are now 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 has in any way suffered a privacy breach. Failure to notify the commissioner of a breach that may pose a real risk of significant harm to individuals 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 harm" must be more than "merely speculative" and not simply "hypothetical or theoretical."

If a breach meets the threshold of being a "real risk of significant harm" and is reported appropriately, the commissioner will then 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.

Outside of Alberta, the current framework for data-breach notifications in the private sector is Canada's federal statute, PIPEDA, which makes data-breach notification voluntary. The federal commissioner has published guidelines and checklists that describe circumstances under which disclosure and notification should be made.

4. Cross-border Transfers and Outsourcing

Cross-border transfers and outsourcing of Canadian personal information to foreign countries have become subjects of focus in Canada. Much of this attention has centred on concerns that U.S. authorities could use the *USA PATRIOT Act* to obtain the personal information of Canadians that is located in or accessible from the U.S. While PIPEDA and related provincial legislation do not prohibit the transfer of personal information outside of Canada, privacy regulators have generally held that notice of such transfers should be provided 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, 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 Canada. 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 now required to notify individuals that they will be transferring individuals' personal information to a service provider outside 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, 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 non-compliance. Under the Alberta PIPA and the British Columbia PIPA, the OPC has the power, following its 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 the OPC can be appealed to the Québec Superior Court.

gowlings: expect innovation, results and value

Founded in 1887, Gowlings is one of Canada's largest law firms, with over 750 professionals in offices across the country and in Moscow, London and Beijing. Recognized for excellence in business, advocacy and intellectual property law, Gowlings provides dedicated industry expertise in the energy, mining, infrastructure, life sciences, government, financial services, technology, manufacturing and distribution sectors, and in areas such as corporate finance and M&A, transfer pricing and tax, patents and trade-marks, and occupational health and safety. For more information, visit

gowlings.com/dbic

This publication is part of Gowlings' *Doing Business in Canada* guide, which provides business executives, foreign counsel and investors with an overview of the legal aspects of Canadian business operations. The information in this guide is current as of September 2011 and is for general information purposes only. It does not constitute a legal opinion or other professional advice.

For further information or to view the rest of the guide, please visit us at gowlings.com/dbic.

montréal • ottawa • toronto • hamilton • waterloo region • calgary • vancouver • beijing • moscow • london • gowlings.com

Gowlings provides legal services in Canada and abroad through the entities Gowling Lafleur Henderson LLP, Gowling Lafleur Henderson S.E.N.C.R.L., s.r.l., Gowlings (UK) LLP, and Gowlings International Inc. In 2011, the firm opened the Gowlings International Inc. Beijing Representative Office. © 2011 Gowlings