Privacy law

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

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 lawsuits 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
2. Employers
3. Reporting privacy breaches
4. Cross-border transfers and outsourcing
5. Enforcement
6. The General Data Protection Regulation

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
- Airports
- Banks
- Broadcasting
- Telecommunications
- Interprovincial railways
- Interprovincial or international trucking, shipping or other forms of transportation
- Nuclear energy
- Offshore drilling operations
- Activities related to maritime navigation

PIPEDA is a privacy law that applies to the collection of personal information regardless of the technology used. This law 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 as well as all interprovincial and international transactions by all organizations subject to PIPEDA in the course of their commercial activities.
In addition, health information custodians - such as physicians, nurses and hospitals - in Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador 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. It should be noted that other Canadian provinces also have health specific legislation that has not been deemed "substantially similar" to PIPEDA; with the effect that both the health specific legislation and PIPEDA may apply even within the province.

b. Provincial

Alberta, British Columbia and Québec have enacted comprehensive private sector privacy legislation, entitled the Personal Information Protection Act (PIPA) in Alberta and British Columbia, 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 employees' personal information. 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 personal information. In most cases, organizations must have either the express or implied consent of the individual in order to collect, use or disclose 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.

According to the Guidelines issued by the Office of the Privacy Commissioner of Canada (the "OPC") on January 1, 2019, obtaining meaningful consent will require greater transparency about how data is collected, used and disclosed. The OPC also has emphasized that "express consent" is the default, and that implied consent will only be appropriate in limited circumstances.

Organizations are required to explain in their privacy policies what personal information is being collected; disclose third parties with whom personal information will be shared; and explain the purposes for which the information is being collected, used and/or disclosed in clear, understandable, and precise terms. Purposes that are integral to provisions of service should be distinguished from those that are not. If presented as "mandatory", the collection, use and disclosure of personal information must be integral to the provision of the product or service. The consumer must be given choices for non-integral collections, uses or disclosures of personal information. Further, organizations must explain the risks of harm and other consequences of residual risks that remain after mitigation measures are put in place.

Organizations must also allow individuals to control the level of detail they get and when, and provide clear options to say yes or no.

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, British Columbia (with regard to certain designated databases), Manitoba, New Brunswick, Newfoundland and Labrador, Nova Scotia, Ontario, Saskatchewan, Prince Edward Island, the Northwest Territories and Yukon have legislation specifically governing the collection, use and disclosure of personal health information. All Canadian provinces and territories have enacted legislation that regulates the collection, use and disclosure of personal information in the public sector. To the extent that private sector organizations are contracting with public bodies and obtaining or receiving personal information that is under the "custody and control" of those public bodies, the public sector legislation will apply to govern the treatment of that information, and the private sector organization should be aware of the potential for "access to information" requests that may impact the information.

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 and 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. It is important to note that 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 Alberta's PIPA and British Columbia's 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 does permit 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

Canada and its provinces have introduced requirements for organizations to proactively notify individuals or the appropriate regulatory bodies of a data breach. PIPEDA, Alberta's PIPA and Health Information Act, New Brunswick's Personal Health Information Privacy and Access Act, Newfoundland and Labrador's Personal Health Information Act, Nova Scotia's Personal Health Information Act, Ontario's Personal Health Information Protection Act, Prince Edward Island's Health Information Act, and the Yukon's Health Information Privacy and Management Act all require mandatory data breach notification.

As of November 1, 2018, PIPEDA requires mandatory breach notification and requires organizations to retain records of all breaches of their security safeguards.

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, (and typically does), direct the organization to notify individuals in the form and manner prescribed by PIPA regulations.

PIPEDA’s breach reporting and notification rules require organizations that experience a data breach to report the incident to the Office of the Privacy Commissioner of Canada and to notify affected individuals, and any other organizations or governments that may reduce the risk of harm. Reporting and notification will be required in all circumstances where it is reasonable to believe that the breach creates a "real risk of significant harm to the individual". Under PIPEDA, "significant harm" is defined to include 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 Act determines the existence of a "real risk of significant harm" by considering 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.

PIPEDA also carries offences for non-compliance with data security breach obligations. 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 focused 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 British Columbia 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 held that notice of such transfers must 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.
In addition, health sector privacy legislation in Newfoundland and Labrador and Nova Scotia imposes restrictions on health information custodians (and organizations that process personal health information on their behalf) with respect to the transfer of personal health information outside the province.

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. This applies whether the third party processor is within Canada or overseas. 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 must 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 the country, and to include information on outsourcing practices in the organization's policies.

The OPC has recently launched a formal consultation process (open until August 6, 2019) on the issue of transfers of information for processing, including cross-border transfers of information between organizations and is considering seeking legislative changes in this regard. The OPC indicated that prior consent may now be required for all "disclosures" of information between organizations, including transfers between organizations and their service providers, and that such transfers may be considered to be a "disclosure" rather than a "use" of the information, which would represent a change in the longstanding guidance from the OPC. The proposal apparently would apply to all transfers, whether made between organizations within Canada or made cross-border, but cross-border transfers appear to be a specific focus of the consultation.

For example, the proposal appears to suggest that in the case of cross-border transfers, the organization must inform the individual of options available to them if they do not wish to have their personal information disclosed across the border, and choices must be made available "for any collection, use or disclosure that is not necessary to provide the product or service." This change in the OPC's position with respect to cross-border data transfers could have a significant impact on organizations doing business in Canada.
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 for 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. The OPC may also begin an investigation where the OPC deems it is warranted, even in the absence of a complaint. 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. There is also the potential for a fine to be imposed for noncompliance with certain provisions of PIPEDA.

Under Alberta's PIPA and British Columbia'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.

The OPC 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 OPC 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.

6. The General Data Protection Regulation

The European Union's ("EU") General Data Protection Regulation ("GDPR") took effect on May 25, 2018. Companies in Canada need to determine whether or not they fall within the scope of the GDPR, and if within the scope, take steps to comply.
The GDPR applies to:

- those with an establishment (subsidiary or branch) in an EU (or European Economic Area ("EEA")) country, in respect of all processing of personal data in that establishment (as controller or processor, as defined by the GDPR); and
- those that do not have an establishment in the EU (or EEA), but which are processing (as controller or processor) personal data of natural persons who are in the EU (or EEA) in relation to the offering goods or services to these persons or the monitoring of their behaviour, with regard to such processing activities only.

Complying with the GDPR means, above all, ensuring that the personal data concerned is processed according to the following principles, subject to any standards adopted by the supervising authority of the relevant country:

- lawfulness, fairness, transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation
- integrity and confidentiality
- accountability

Learn more about Gowling WLG services in privacy law »

NOT LEGAL ADVICE. Information made available on this website in any form is for information purposes only. It is not, and should not be taken as, legal advice. You should not rely on, or take or fail to take any action based upon this information. Never disregard professional legal advice or delay in seeking legal advice because of something you have read on this website. Gowling WLG professionals will be pleased to discuss resolutions to specific legal concerns you may have.