DATA PROTECTION LAWS OF THE WORLD

Canada

DLA PIPER

CANADA

Last modified 28 January 2021

LAW

In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, criminal code provisions etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information.

The summary below focuses on Canada's private sector privacy statutes:

- Personal Information Protection and Electronic Documents Act ('PIPEDA')
- Personal Information Protection Act ('PIPA Alberta')
- Personal Information Protection Act ('PIPA BC')
- Personal Information Protection and Identity Theft Prevention Act ('PIPITPA') (not yet in force)
- An Act Respecting the Protection of Personal Information in the Private Sector ('Quebec Privacy Act'), (collectively, 'Canadian Privacy Statutes')

PIPEDA is expected to be replaced by a new federal statute sometime in 2021 or 2022 - the Consumer Privacy Protection Act ('CPPA'), which has been introduced in Canada's Parliament and will undergo continued debate. The CPPA, as currently drafted, will provide additional rights to data subjects (e.g. portability of data), expands the requirements for valid data subject consent, and sets out monetary penalties of up to 5% of annual global revenue.

PIPEDA applies to all of the following:

- Consumer and employee personal information practices of organizations that are deemed to be a 'federal work, undertaking or business' (eg banks, telecommunications companies, airlines, railways, and other interprovincial undertakings)
- Organizations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province, unless the province has enacted 'substantially similar' legislation (PIPA BC, PIPA Alberta and the Quebec Privacy Act have been deemed 'substantially similar')
- Inter provincial and international collection, use and disclosure of personal information in connection with commercial activity

PIPA BC, PIPA Alberta and the Quebec Privacy Act apply to both consumer and employee personal information practices of organizations within BC, Alberta and Quebec, respectively, that are not otherwise governed by PIPEDA.

DEFINITIONS

Definition of personal data

'Personal information' includes any information about an identifiable individual (business contact information is expressly "carved

out" of the definition of 'personal information' in some Canadian privacy statutes.

Definition of sensitive personal data

Not specifically defined.

NATIONAL DATA PROTECTION AUTHORITY

- Office of the Privacy Commissioner of Canada ('PIPEDA')
- Office of the Information and Privacy Commissioner of Alberta ('PIPA Alberta')
- Office of the Information and Privacy Commissioner for British Columbia ('PIPA BC'), and
- *Commission d'accès à l'information du Québec* ('Quebec Privacy Act')

REGISTRATION

There is no registration requirement under Canadian Privacy Statutes.

DATA PROTECTION OFFICERS

PIPEDA, PIPA Alberta, PIPA BC and PIPITPA expressly require organizations to appoint an individual responsible for compliance with the obligations under the respective statutes.

COLLECTION & PROCESSING

Canadian Privacy Statutes set out the overriding obligation that organizations only collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Subject to certain limited exceptions prescribed in the Acts, consent is required for the collection, use and disclosure of personal information. Depending on the sensitivity of the personal information, consent may be opt in or opt out. Organizations must limit the collection of personal information to that which is necessary to fulfil the identified purposes and only retain such personal information for as long as necessary to fulfil the purposes for which it was collected.

Each of the Canadian Privacy Statutes have both notice and openness/transparency requirements. With respect to notice, organizations are generally required to identify the purposes for which personal information is collected at or before the time the information is collected. With respect to openness/transparency, generally Canadian Privacy Statutes require organizations make information about their personal information practices readily available.

All Canadian Privacy Statutes contain obligations on organizations to ensure personal information in their records is accurate and complete, particularly where the information is used to make a decision about the individual to whom the information relates or if the information is likely to be disclosed to another organization.

Each of the Canadian Privacy Statutes also provides individuals with the following:

- A right of access to personal information held by an organization, subject to limited exceptions
- A right to correct inaccuracies in/update their personal information records.

Finally, organizations must have policies and practices in place that give effect to the requirements of the legislation and organizations must ensure that their employees are made aware of and trained with respect to such policies.

TRANSFER

When an organization transfers personal information to a third party service provider (ie who acts on behalf of the transferring organization), the transferring organization remains accountable for the protection of that personal information and ensuring compliance with the applicable legislation. In particular, the transferring organization is responsible for ensuring that the third party service provider appropriately safeguards the data, and would also be required under the notice and openness/transparency provisions to reference the use of third party service providers in and outside of Canada in their privacy policies and procedures.

With respect to the use of foreign service providers, PIPA Alberta specifically requires a transferring organization to include the following information in its privacy policies and procedures:

- The countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and
- The purposes for which the third party service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization

Under PIPA Alberta, specific notice must also be provided at the time of collection or transfer of the personal information and must specify:

- The way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and
- The name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization.

In addition, under the Quebec Privacy Act, an organization must take reasonable steps to ensure that personal information transferred to service providers outside Quebec will not be used for other purposes and will not be communicated to third parties without consent (except under certain exceptions prescribed in the Act). The Quebec Privacy Act also specifically provides that the organization must refuse to transfer personal information outside Quebec where it does not believe that the information will receive such protection.

SECURITY

Each of the Canadian Privacy Statutes contains safeguarding provisions designed to protect personal information. In essence, these provisions require organizations to take reasonable technical, physical and administrative measures to protect personal information against loss or theft, unauthorized access, disclosure, copying, use, modification or destruction. These laws do not generally mandate specific technical requirements for the safeguarding of personal information.

BREACH NOTIFICATION

Currently, PIPEDA, PIPA Alberta and PIPITPA are the only Canadian Privacy Statute with breach notification requirements.

In Alberta, an organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result.

Notification to the Commissioner must be in writing and include:

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date or time period during which the loss or unauthorized access or disclosure occurred
- A description of the personal information involved in the loss or unauthorized access or disclosure
- An assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure
- An estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
- A description of any steps the organization has taken to reduce the risk of harm to individuals
- A description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure, and
- The name and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss of unauthorized access or disclosure

Where an organization suffers a loss of or unauthorized access to or disclosure of personal information as to which the organization is required to provide notice to the Commissioner, the Commissioner may require the organization to notify the individuals to whom there is a real risk of significant harm. This notification must be given directly to the individual (unless specified otherwise by the Commissioner) and include:

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date on which or time period during which the loss or unauthorized access or disclosure occurred
- A description of the personal information involved in the loss or unauthorized access or disclosure
- A description of any steps the organization has taken to reduce the risk of harm, and
- Contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure

The breach notification provisions under PIPEDA are very similar to the breach notification provisions under PIPA Alberta. Under PIPEDA, organizations must also keep a record of ALL information security breaches, even those which do not meet the risk threshold of a "real risk of significant harm".

In Manitoba, PIPITPA (which is not yet in force) provides that an organization must, as soon as reasonably practicable, notify an individual if personal information about the individual that is in its custody or under its control is stolen, lost or accessed in an unauthorized manner. This requirement to notify an individual does not apply where:

- The organization is instructed to refrain from doing so by a law enforcement agency that is investigating the theft, loss or unauthorized accessing of the personal information, or
- The organization is satisfied that it is not reasonably possible for the personal information to be used unlawfully

The exact form of the notice that must be provided to individuals has not yet been prescribed.

ENFORCEMENT

Privacy regulatory authorities have an obligation to investigate complaints, as well as the authority to initiate complaints.

Under PIPEDA, a complaint must be investigated by the Commissioner and a report will be prepared that includes the Commissioner's findings and recommendations. A complainant (but not the organisation subject to the complaint) may apply to the Federal Court for a review of the findings and the court has authority to, among other things, order an organisation to correct its practices and award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Under PIPA Alberta and PIPA BC, an investigation may be elevated to a formal inquiry by the Commissioner resulting in an order. Organisations are required to comply with the order within a prescribed time period, or apply for judicial review. In both BC and Alberta, once an order is final, an affected individual has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the breach.

In Alberta and BC, a person that commits an offence may be subject to a fine of not more than CA$100,000. Offences include, among other things, collecting, using and disclosing personal information in contravention of the Act (in Alberta only), disposing of personal information to evade an access request, obstructing the commissioner, and failing to comply with an order.

Similarly, under the Quebec Privacy Act, an order must be complied with within a prescribed time period. An individual may appeal to the judge of the Court of Quebec on questions of law or jurisdiction with respect to a final decision.

A failure to comply with the Quebec Privacy Act's requirements in respect of the collection, storage, communication or use of personal information is liable to a fine of up to CA$10,000 and, for a subsequent offence, to a fine up to CA$20,000. Any one who hampers an inquiry or inspection by communicating false or inaccurate information or otherwise is liable to a fine of up to CA$10,000 and, for a subsequent offence, to a fine of up to CA$20,000.

Under the PIPITPA, it is an offence to (a) willfully collect, use, or disclose personal information in contravention of the Act, (b) wilfully attempt to gain or gain access to personal information in contravention of the Act, and (c) dispose of or alter, falsify, conceal or destroy personal information or any record relating to personal information, or direct another person to do so, with an intent to evade a request for access to information or the record. A person who commits an offence is liable on summary conviction, in the case of a person other than an individual, to a fine of not more than CA$100,000.

ELECTRONIC MARKETING

Electronic marketing is governed by both Canadian Privacy Statutes (as discussed above), as well as Canada's Anti-Spam Legislation (CASL).

Under CASL it is prohibited to send, or cause or permit to be sent, a commercial electronic message (defined broadly to include text, sound, voice, or image messages aimed at encouraging participation in a commercial activity) unless the recipient has provided express or implied consent and the message complies with the prescribed content and unsubscribe requirements (subject to limited exceptions).

What constitutes both permissible express and implied consent is defined in the Act and regulations. For example, an organization may be able to rely on implied consent when there is an existing business relationship with the recipient of the message, based on:

- A purchase by the recipient within the past two years, or
- A contract between the organization and the recipient currently in existence or which expired within the past two years

CASL also prohibits the installation of a computer program on any other person's computer system, or having installed such a computer program to cause any electronic messages to be sent from that computer system, without express consent, if the relevant system or sender is located in Canada. In addition, the Act contains anti phishing provisions that prohibit (without express consent) the alteration of transmission data in an electronic message such that the message is delivered to a destination other than (or in addition to) that specified by the sender.

CASL also introduced amendments to PIPEDA that restrict 'address harvesting', or the unauthorized collection of email addresses through automated means (*ie*, using a computer program designed to generate or search for, and collect, email addresses) without consent. The use of an individual's email address collected through address harvesting also is restricted.

The 'Competition Act' was also amended to make it an offence to provide false or misleading representations in the sender information, subject matter information, or content of an electronic message.

CASL contains potentially stiff penalties, including administrative penalties of up to CA$1 million per violation for individuals and CA$10 million for corporations (subject to a due diligence defense). CASL also sets forth a private right of action permitting individuals to bring a civil action for alleged violations of CASL (CA$200 for each contravention up to a maximum of CA$1 million each day for a violation of the provisions addressing unsolicited electronic messages). However, the private right of action is not yet in force.

ONLINE PRIVACY

Online privacy is governed by Canadian Privacy Statutes (discussed above). In general, Canadian privacy regulatory authorities have been active in addressing online privacy concerns.

For example, in the context of social media, the OPC has released numerous Reports of Findings addressing issues including:

- Default privacy settings
- Social plug-ins
- Identity authentication practices
- The collection, use and disclosure of personal information on social networking sites. The OPC has also released decisions and guidance on privacy in the context of Mobile Apps

In addition, the OPC has released findings and guidelines related to the use of cookies and online behavioral advertising, including findings indicating that information stored by temporary and persistent cookies is considered to be personal information and therefore subject to PIPEDA. The OPC has adopted the same position with respect to information collected in connection with online behavioral advertising.

In 'Privacy and Online Behavioral Advertising' (the 'OBA Guidelines'), the OPC stated that it may be permissible to utilize opt-out consent in the context of online behavioral advertising if the following conditions are met:

- Individuals are made aware of the purposes for the online behavioral advertising, at or before the time of collection, in a manner that is clear and understandable

- Individuals are informed of the various parties involved in the online behavioral advertising at or before the time of collection
- Individuals are able to opt-out of the practice and the opt-out takes effect immediately and is persistent
- The information collected is non-sensitive in nature (*ie*, not health or financial information), and
- The information is destroyed or made de-identifiable as soon as possible

The OPC has indicated that online behavioral advertising must not be a condition of service and, as a best practice, should not be used on websites directed at children.

With respect to location data, such information, whether tied to a static location or a mobile device, is considered to be personal information by Canadian privacy regulatory authorities. As such, any collection, use or disclosure of location data requires, among other things, appropriate notice and consent. Most of the privacy regulatory authority decisions related to location data have arisen with respect to the use of GPS in the employment context.

The Canadian privacy regulatory authorities provide the following test that must be met for the collection of GPS data (and other types of monitoring and surveillance activities):

- Is the data demonstrably necessary to meet a specific need?
- Will the data likely be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Are there less privacy-intrusive alternatives to achieve the same objective?

KEY CONTACTS

Tamara Hunter
Associate Counsel
T +1 604.643.2952
tamara.hunter@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.