CASSELS BROCK
LAWYERS

Privacy Law

Doing Business In Canada

Does Canada Have Privacy Legislation?

Federal Legislation

Canada has a comprehensive legal framework that governs the collection, retention, use and disclosure of the personal information of identifiable individuals in both the public and private sectors. Described as a middle ground between the European privacy regime and the US regulatory framework, the federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") applies generally to the collection, use and disclosure in the course of commercial activities in the private sector.

Personal information under PIPEDA means any information about an identifiable individual other than such person's "business card" information — that is, the name, title, business address or telephone number of the employee in question. An individual's business email address is currently considered personal information under PIPEDA.

Federal Privacy Guidelines

PIPEDA is based on a set of privacy guidelines that were developed by the Canadian Standards Association that may be summarized as follows:

- Accountability of the organization that has personal information under its control;
- Identification of the purpose for which the information is collected;
- Consent from the individual whose personal information is being collected, used or disclosed;
- Limitation of the personal information collected — and the use, disclosure and retention of personal information — to that which is necessary for the identified purpose;
- Accuracy, thoroughness and currency of the personal information for the identified purpose;
- Protection of personal information via safeguards;
- Openness of an organization's policies and practices concerning personal information management;
- Access to (and the opportunity to challenge the accuracy and completeness of) personal information that has been collected, used and/or disclosed about an individual by that individual; and
- The opportunity to challenge an organization's compliance with these principles.

Recognition of PIPEDA

With limited reservations, the European Union has recognized PIPEDA as providing an adequate level of protection for personal data transferred from the European Community to Canada. For personal information sent to organizations in Canada that are *not* subject to PIPEDA, the EU's "standard contractual clauses" must be used.

Federal and Provincial Jurisdiction

Since Canada's Constitution provides that labour and employment are matters over which the provinces have jurisdiction (and not the federal government), PIPEDA only applies to the collection, use and disclosure of the personal information of employees of *federal works, undertakings, or businesses*. Three Canadian provinces — Alberta, British Columbia and Québec — have broad private sector privacy legislation presently in force. Organizations operating in those provinces are exempt from PIPEDA compliance concerning the collection, use and disclosure of personal information occurring *within* each of those provinces. Where both the federal and provincial legislation apply, compliance with both applicable statutes may be required, depending on the circumstances.

Current as of September 2015

Provincial Legislation

The provincial statutes are implicitly (if not explicitly) modelled on the same type of privacy principles as PIPEDA.

Ontario Privacy Legislation

Although Ontario did not pass an equivalent to PIPEDA, it did enact the *Personal Health Information Protection Act, 2004* ("**PHIPA**"). "Health information custodians," as defined in PHIPA, are exempt from the application of Part I of PIPEDA regarding the collection, use and disclosure of personal health information occurring within the province.

Ontario also enacted both the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*. These statutes contain provisions intended to protect personal information collected by provincial and municipal governments and provide the means to access government records. Similar legislation has been enacted in all of the other provinces. The *Privacy Act* and *Access to Information Act* provide similar rights at the federal level.

Alberta and British Columbia Privacy Legislation

The Alberta and British Columbia private sector privacy statutes — each of which is entitled the *Personal Information Protection Act* ("**PIPA**") — were enacted at the same time and are very similar (although not identical) in structure and language.

Personal Information Definitions

While both PIPA statutes use the term "personal information," the BC statute specifically excludes contact information from the definition (i.e., information to enable an individual at a place of business to be contacted including the name, position name or title, business telephone number, business address, business email or business fax number of the individual). The BC legislation also excludes work product information (i.e., information prepared or collected by an individual(s) as a part of his or her responsibilities or activities related to his, her, their or its employment or business, but not including information about an individual who did not prepare or collect the information).

Business Transaction Exemption

Both the Alberta and BC PIPA statutes permit parties to a business transaction to collect, use and disclose personal information necessary to determine whether to proceed with the transaction, and to complete the transaction without the consent of the affected individual(s). The parties may so collect, use and disclose provided that they have entered into a form of non-disclosure agreement restricting the use and disclosure of the information to the purposes related to the business transaction. The BC statute also obligates the parties to notify affected individuals that the transaction has occurred and that their personal information has been disclosed to the other party.

Employee Information

The Alberta PIPA statute defines "personal employee information" while the BC PIPA statute defines "employee personal information." In both cases, any information reasonably required to establish, manage or terminate an employment relationship can be collected, used or disclosed *without* consent. However, in Alberta, "employee" is defined to include potential, current or former employees and volunteers and "personal employee information" also includes information reasonably required to manage a post-employment or post-volunteer-work relationship. Under the BC legislation, the term is arguably more restrictive in that it refers to personal information about an individual that is collected, used or disclosed *solely* for the purposes reasonably required to establish, manage or terminate an employment relationship.

Alberta-Specific Provisions

Service Providers Outside of Canada

The Alberta PIPA statute contains a special provision whereby certain notices must be provided to individuals at the time of collection of their personal information if a service provider outside of Canada is used to either collect personal information or if personal information is to be transferred to a service provider outside of Canada.

Where any incident involving the loss of (or unauthorized access to or disclosure of) personal information occurs, and a reasonable person would consider that a real risk


of significant harm to an individual exists as a result of such incident, the Alberta Information and Privacy Commissioner must be notified of such loss, unauthorized access or disclosure.

Non-Profit Organizations

The Alberta PIPA statute exempts "non-profit organizations" from compliance unless personal information is being collected, used or disclosed by the non-profit organization in connection with a commercial activity (as defined in the statute).

Status of PIPA Legislation

The current status of the Alberta PIPA is uncertain. In 2013, the Supreme Court of Canada declared the legislation was unconstitutional but suspended its declaration of invalidity for one year so that the province could pass remedial legislation. As of the date hereof, Alberta has yet to pass any amendments or a new law to do so.

Québec Privacy Legislation

The Québec *Act Respecting the Protection of Personal Information in the Private Sector* (the "**APPIPS**") predates PIPEDA by several years and, although based on similar privacy principles, is quite different in its structure and language. The APPIPS covers all persons carrying on a business in the Province of Québec including individuals who sell goods and services, partnerships and associations. The Act regulates the collection, holding, use and communication of personal information and, similar to PIPEDA, provides a procedure whereby a person may access a file held by a business about him or her and obtain rectification of any inaccurate, incomplete or equivocal information contained therein.

Whereas, under PIPEDA, consent must be an informed consent, in the Province of Québec, s. 14 of the APPIPS requires that consent be "manifest, free, and enlightened"; however, similar to PIPEDA, the consent is given for specific disclosed purposes. Such consent is valid only for the length of time needed to achieve the purposes for which is was requested. Consent given other than in accordance with these requirements is without effect.

Manitoba Privacy Legislation

The Province of Manitoba enacted the *Personal Information Protection and Identity Theft Prevention Act* (PIPITPA) in 2013. This statute, which is very similar to Alberta's (currently unconstitutional) legislation, has not yet been proclaimed in force.

How Does Canada's Privacy Legislation Compare with Privacy Legislation in Other Jurisdictions?

Right to Privacy

The right to privacy is not enshrined as a fundamental freedom in the *Canadian Charter of Rights and Freedoms*. However, the protection of personal information (as discussed above) is recognized by statute. Certain provinces have statutorily created a tort of invasion of privacy. Whether such a tort exists at common law in Canada remains unsettled. In Ontario, the tort of "intrusion upon seclusion" has been recognized.

No data controller or processor

Canadian privacy law does not employ the concepts of "data controller" or "data processor"; it simply refers to the collection, use and disclosure of personal information by organizations in the course of commercial activities. Obligations imposed at the time of collection would be the responsibility of the organization performing the collection, and the collecting organization must ensure that any other organizations to which it may provide this information for processing also comply with these obligations. Similarly, there is no requirement in the federal or provincial privacy legislation to register with any Canadian federal or provincial government entity as a data controller, or to notify any Canadian federal or provincial government body of any data processing.

Transfer of Information Outside of Canada

While neither PIPEDA, the private sector provincial privacy legislation, nor most of the public sector provincial privacy laws prohibit the transfer of personal information outside of Canada, certain provincial statutes applicable to the public sector do contain this prohibition. Nonetheless,


there has been a great deal of discussion in Canada about the transfer of personal information to the United States and the implications of the *USA PATRIOT Act*. Where personal information is transferred out of Canada, the generally accepted best practice is to notify the individual in advance that his or her information may be subject to government access by lawful authorities in the recipient foreign jurisdiction.

Order-making Authority

Canada's federal privacy commissioner does not have order-making authority. He or she is compelled to investigate complaints and issue reports, but may not order any particular action or impose any financial penalties. Privacy commissioners at the provincial level do have order-making authority.

Mandatory Breach Notification

Unlike the laws of many other jurisdictions, PIPEDA does not contain any mandatory breach notification provisions; however, the federal Bill S-4, known as the "*Digital Privacy Act*," would introduce a number of amendments to PIPEDA, including a breach notification provision.

Anti-Spam Legislation

Canada's anti-spam legislation ("**CASL**") came into force on July 1, 2014. CASL affects how businesses and organizations communicate with Canadians to encourage participation in a commercial activity through the use of "commercial electronic messages" ("**CEMs**") i.e., emails, text messages, instant messages, social media messages and other non-broadcast electronic communications, but not telephone calls, voice mails or faxes. CASL also affects how Canadians communicate electronically with the rest of the world.

Disclosure and Consent

Organizations and individuals are prohibited from sending CEMs without first disclosing certain identity, location and unsubscribe information about the sender (including additional disclosure where CEMs are sent on behalf of an affiliate or third party) and obtaining the express, informed, opt-in, consent of the recipient unless consent can be implied or an exclusion applies. CEMs must comply with message format and unsubscribe notification requirements.

Implied Consent

Implied consent may be found where there is an existing business relationship between the sender and recipient (who could be an individual). Such a relationship generally arises:

- From the purchase of a good, service, investment or interest in land, or a contract, and is generally valid for a two-year period;
- From certain types of volunteer, charitable and political activities or from membership in certain types of clubs, associations and voluntary organizations, and is also generally valid for a two-year period;
- Where the recipient's email address has been conspicuously published without an accompanying anti-spam notice and the CEM is related to the recipient's business, role or official functions; or
- Where the recipient has disclosed his or her email address to the sender without indicating that he or she does not want to receive CEMs at that address and the CEM is related to the recipient's business, role or official functions.

Even where there is implied consent to its transmission, the CEM must still contain the sender's identity, location and contact information and a clear unsubscribe mechanism (as well as additional disclosure where the CEM is sent on behalf of an affiliate or third party).

Full and Partial CASL Exemptions

Key full exemptions from CASL compliance include (but are not limited to) CEMs that:

- Are completely non-commercial in nature;
- Are sent to another organization (not an individual) with whom the sender has a relationship and are relevant to the recipient organization's activities;
- Inquire about (or make an application concerning) the recipient's commercial activity;
- Respond to requests, enquiries or complaints received from the recipient;
- Are sent to satisfy various legal/juridical obligations or notice requirements or enforce legal rights;
- Are sent among an organization's representatives and concern the organization's activities; or
- Are sent to a scheduled foreign state and comply with the foreign state's spam law that targets "substantially similar" conduct.


Key partial exemptions include CEMs that:

- Facilitate, complete, or confirm a commercial transaction;
- Provide information about the employment relationship or benefit plans with a currently participating person; or
- Deliver or provide a quote/estimate, warranty, product recall or safety/security or factual information concerning ongoing use/purchase of a product, good or service (including updates and upgrades) in certain circumstances.

CEMs that fall under a *partial* exemption must still contain the sender's identity, location and contact information and a clear unsubscribe mechanism (as well as additional disclosure where the CEM is sent on behalf of an affiliate or third party).

Penalties for Non-compliance

Penalties for non-compliance where CASL applies include:

- Significant Administrative Monetary Penalties;
- Potential personal liability for the organization's directors and officers, and
- As of 2017, a private right of action.

Although a due diligence defence is available, to rely upon this defence senders must show that they have taken steps to bring their electronic communication practices into compliance with CASL, including establishing clear documentation trails.

CASSELS BROCK
LAWYERS

Cassels Brock & Blackwell LLP
Toronto | Vancouver | Calgary
casselsbrock.com