



Ariane Siegel, Partner
Business Law
Toronto
(416) 369-7228
ariane.siegel@gowlings.com

Ariane is a member of the Firm's Technology Practice Group. She has a specialized background in commercial law and in regulatory and policy matters pertaining to the communications industry. She regularly advises on privacy, e-commerce and telecom matters for the retail industry, financial services companies and the technology sector. Ariane is co-leader of the American Bar Association subcommittee on privacy.

An Overview of Privacy Law in Canada: Important Tips for Businesses

Ariane Siegel

As of January 1, 2004, Canadian businesses must comply with the *Protection of Personal Information and Electronic Documents Act* (PIPEDA) and similar legislation in various provinces (Québec, Alberta, B.C. and Ontario in respect of personal health information). PIPEDA protects individuals' personal information and its use in the course of commercial activities. Depending on an organization's activities and use of personal information, compliance can be as simple as preparing privacy policies, or it can involve complex processes, such as staff training, storage system improvements and implementing protective measures.

Privacy issues will likely affect an organization or company in two ways:

1. An organization will have to comply with PIPEDA with respect to the collection and control of customers' personal information. Federal works and undertakings and organizations with employees in B.C., Alberta or Québec must also consider the impact of provincial privacy laws on the collection of employees' personal information.
2. An organization's partners (who must also comply with privacy obligations) will want to ensure that they safeguard the personal information accessed while performing services.

The following brief overview of privacy legislation in Canada is not intended as legal advice, but an introduction to relevant compliance issues.

Overview of PIPEDA

PIPEDA balances an individual's right to privacy and the need of businesses to make reasonable use of personal information. "Personal information" is defined as "information about an identifiable individual." It does not include an employee's name, title, business address or telephone number. It includes information such as race; ethnic origin; colour; age; marital status; religion; education; medical; criminal; employment or financial history; address; telephone number; Social Insurance Number; fingerprints; blood type; tissue or biological sample; views or personal opinions.

PIPEDA applies to organizations in Canada that collect, use or disclose personal information in the course of any commercial activity, defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character."

PIPEDA is not a long-arm statute and, until recently, it was commonly thought that it applied only to organizations with a place of business or employees

in Canada. However, a recent decision by the Federal Court of Canada suggests that the Federal Privacy Commissioner has the right to investigate any organization, regardless of existing Canadian infrastructure, that collects, uses or discloses personal information. In *Philippa Lawson v. Accusearch Inc. DBA Abika.com and The Privacy Commissioner of Canada*, it was held that PIPEDA gives the Privacy Commissioner jurisdiction to investigate complaints relating to the transborder flow of personal information. The scope of PIPEDA, combined with provincial consumer protection acts, raises important issues for companies without Canadian infrastructure that offer online services.

What does an organization need to do?

PIPEDA outlines 10 primary principles for protecting personal information. Organizations should follow them closely and ensure they are reflected in any policies and procedures.

The most important principle is the need to obtain consent when personal information is collected, used or disclosed. PIPEDA also requires that personal information be used or disclosed for the purposes for which it was collected. Once an organization collects personal information, it must fulfill certain obligations with respect to its use and safeguarding.



They must:

- **Be accountable:** An organization must be responsible for personal information under its control and designate an individual or individuals accountable for compliance.
- **Identify the purpose:** The purpose for which personal information is collected shall be identified by the organization during or before collection.
- **Obtain consent:** The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.
- **Limit use, disclosure and retention:** Personal information must not be used or disclosed for purposes other than those for which it was collected, unless explicit consent has been received, or by legal requirement. Information may only be retained as long as needed to fulfill those purposes.
- **Be accurate:** Personal information must be accurate, complete and up-to-date.
- **Use appropriate safeguards:** Personal information must be protected by security safeguards to protect the sensitivity of the information.
- **Be open:** An organization will make its personal information management policies and practices readily available.
- **Give individuals access:** Upon request, an individual shall be informed of the existence, use and disclosure of his or her own personal information and be given appropriate access. An individual can challenge the accuracy and completeness of the information and have it amended as appropriate.
- **Provide recourse:** An individual can challenge an organization's compliance with the above principles and seek recourse from the individuals responsible for the organization's compliance.

What are the risks if an organization does not comply?

PIPEDA allows individuals to complain about an organization's non-compliance with personal information policies. These complaints are heard by the Federal Privacy Commissioner, who receives, investigates and resolves disputes and complaints. Provincial complaints are heard by provincial privacy commissioners.

The Privacy Commissioner may also make public information relating to an organization's personal information management practices, if it is deemed in the public's interest. The public disclosure of complaints, as a consequence of misusing personal information, can be very damaging to a business. The individual filing the complaint can also apply to the courts for:

- Damages (a monetary award);
- An order compelling the organization to correct its practices; and/or
- An order compelling the organization to make public a notice of any action taken or proposed to correct its practices.

PIPEDA also creates offences for the following activities:

- Obstructing an investigation or audit;
- Destroying personal information that is the subject of an access request; or
- Disciplining a whistle-blower.

An organization that engages in these activities can be fined up to \$10,000 for a summary conviction or \$100,000 for an indictable offence.

Processing of personal information in the United States

Organizations are obliged to safeguard personal information processes and not disclose information to third parties without consent. This has led to issues connected with the outsourcing of data management services. An organization that offers services, or

stores data it processes, outside of Canada should be aware of these issues. In addition, some provinces impose restrictions on the outsourcing of personal information held by government organizations. Many concerns can be dealt with through data protection agreements, combined with appropriate notice requirements.

Data breach notification in Canada

Although neither PIPEDA nor similar statutes in B.C., Alberta or Québec require a mandatory breach notification, there are guidelines on data breach notification in effect at the federal and provincial levels, and organizations are strongly advised to follow them. The Office of the Privacy Commissioner has made detailed information on breach notification available on its website. Visit www.privcom.gc.ca for details.



In Canada, Ontario's PHIPA is currently unique in imposing mandatory breach notification: health information custodians are required to notify individuals whose personal health information has been inappropriately handled.

It is expected that the federal government will amend PIPEDA to provide for some form of breach notification in the near future.