ALBERTA efuturecentre

Internet Privacy

An initiative of:

THE BUSINESSLINK Business Service Centre

Funded by:

Western Economic Diversification Canada | Diversification de l'économie de l'Ouest Canada | Canada

Introduction

Privacy is often defined as the right to be left alone, or the right to not have information about you collected, or used or disclosed without your consent.

In recent years, privacy has become a hot topic. Governments around the world have reacted by introducing new laws to deal with real or perceived dangers arising from digital and computer technologies and the ability to process and organize data in new ways.

Privacy on the Internet is of particular concern given the ability to not only collect personal information, often without your knowledge, but also to transfer it around the world. There is a broad consensus that personal information (defined as information about an identifiable individual) is at risk, and that legal and other means are necessary to protect individual privacy rights.

Interestingly, only individuals have privacy rights; corporations and other organizations do not. Corporations may have rights, however, to confidentiality of information under a non-disclosure agreement, for example, or as part of an employment contract.

The OECD and European Laws – Why They Matter

As far back as the early 1980s, the Organization for Economic Cooperation and Development, a group of 30 countries committed to democratic government and free market economies, reacted to the increasing use of computers and databases by developing a model privacy code for organizations to use. For more information, click on www.oecd.org.

During the 1990s, the European Union developed and enacted its Privacy Directive, also known as the EU Data Protection Directive, which was designed to protect the personal information of European citizens. One of the provisions of the Directive was that European organizations could not share personal information with organizations in other countries, unless these countries had adequate laws protecting individual privacy. You can read the Directive at the following Internet address: http://europa.eu.int/comm/internal_market/privacy/index_en.htm.

10 Principles of PIPEDA

Partly in response to the European Directive, Canada enacted the Personal Information Protection and Electronic Documents Act (PIPEDA), which came into effect in stages starting in 2001. As of January 1, 2004, in its final stage, PIPEDA applies to all commercial activities carried out by Canadian organizations, both provincially and internationally. "Organization" refers not only to societies and corporations, but also to you as an individual if you are carrying on business and engaging in commercial activities.

PIPEDA does state that organizations in certain provinces may be declared exempt from the provisions of PIPEDA if these provinces have enacted substantially similar laws to PIPEDA. To date, BC, Alberta and Quebec have done so and have been declared exempt from PIPEDA by the federal government. However, this only applies to activities within those provinces; cross-border activities may still be subject to PIPEDA. Also, federally regulated organizations such as banks, airlines and telecommunications companies have always been, and continue to be, subject to PIPEDA.

PIPEDA incorporates the provisions of the CSA (Canadian Standards Association) model code, which consists of ten "fair information principles." The ten principles can be summarized as follows:

1. **Accountability** – Organizations must designate an individual or individuals who will be responsible for complying with PIPEDA. Their contact information must be publicly accessible as well. Such person(s) will be legally responsible for protecting all personal information held by the organization or information subject to transfer to a third party. Taking on this role is not something to be taken lightly. Your "Privacy Officer," which is a typical title for this individual, should also have sufficient authority to carry out their role and duties.

2. **Identifying the purposes** – Organizations must identify the reasons for collecting personal information at or before the time of collection and the purposes for which the information will be used and disclosed. This means

clearly identifying the business processes involved and their purposes. You should write them down so that they are clear.

3. **Obtaining consent** – There are some exemptions in the law. However, unless an exemption is available, consent of the individual must be obtained at or before the time of collection and again if a new use for the personal information is identified. This applies to situations where information about an individual is being obtained from third parties or directly from the individual. There is some ability to use opt-out consent mechanisms in certain cases where you can assume consent unless the person tells you otherwise, but you should be careful with these methods.

4. **Limiting collection** – Personal information can be collected only to the extent necessary for the identified and stated purposes. You cannot over-collect.

5. **Limiting use, disclosure and retention** – Organizations must put guidelines and procedures into place on how they use, disclose and retain personal information. The use, disclosure and retention must also be limited to that required by the stated purposes. This means that if you cannot justify a particular practice or procedure, you should not be doing it.

6. **Ensuring and maintaining accuracy** – Organizations are responsible for minimizing the possibility of using incorrect or outdated personal information. Your information should be up to date, especially if you are using it to make decisions about people.

7. **Providing adequate security** – Adequate measures must be taken to protect personal information against loss or theft, unauthorized access, disclosure, copying, use, destruction or modification. This includes not only network security keeping the data secure from hackers and similar threats but also physical security, such as locked doors, and restricted access to only those individuals who need to know.

8. **Making information management policies readily available** – Organizations must have written privacy policies, procedures and practices, and must make these policies easy to understand and available to the public.

9. **Providing individuals with access to information about themselves** – Generally individuals are to be given access to any personal information concerning them in your custody or control if requested. There are types of information, however, that you can refuse to provide, such as certain types of confidential information, and there are types of information you cannot legally provide, such as personal information about someone else.

10. **Giving individuals the right to challenge compliance** – Organizations must develop simple and easily accessible complaint procedures. They must investigate all complaints received, and they must take appropriate measures to correct information-handling practices and policies in light of valid complaints.

If you understand these principles, you already know a great deal about privacy law. For further information, you can visit the website of the Privacy Commissioner of Canada at www.privcom.gc.ca.

It is also important to keep in mind that privacy laws do not just apply to online business; they are equally applicable in the world of paper and filing cabinets as well.

Provincial Laws

A number of provinces in Canada have their own laws with respect to privacy:

- Quebec, in fact, had the first privacy law in North America, passed in 1994.
- Alberta and BC have very similar laws, both called the Personal Information Protection Act, or PIPA.
- The provisions of all these laws are very similar to PIPEDA, although they are organized differently.
- In addition, BC, Saskatchewan, Manitoba and Quebec have laws that make an invasion of privacy a tort. A tort is a civil wrong that gives you the right

to sue for damages. Therefore, in these four provinces, a person affected by your invasion of their privacy may have a right to sue you for damages.

There is also a provision in the Criminal Code of Canada, which has never been tested in court, that could make intercepting and reading the e-mail or web surfing habits of others, for example your employees, an illegal wire-tap subject to criminal penalties, unless you obtain the consent of at least one party involved in the communication or a court order.

Alberta Law - PIPA

If you are based in Alberta, and particularly if you carry out the processing of personal information in Alberta, you will almost certainly be subject to Alberta's PIPA. In your online activities, you may also be subject to PIPEDA, as well as the privacy laws of other countries, depending on what personal information you collect, use or disclose and where the individuals in question are located. For example, if you collect personal information about residents of Manitoba, or California, or even England or France, you may be subject to the laws of those countries. If you are located in Alberta or process the information in Alberta, you will also almost certainly be subject to PIPA. This is a very complex area that you may want to discuss with a lawyer.

Laws of Other Countries

It is important to understand that you cannot ignore the laws of other countries just because you are not physically there. This is a complicated area of the law. You should keep in mind, however, that:

- Serious breaches of the laws of another country may allow that country to have you arrested in Canada and extradited (meaning you are transported to the other country to face charges
- It may be possible for parties in the other country to sue you for damages here in Canada
- Canadian courts may recognize and enforce the judgments of courts in other countries in certain cases

Online Issues

In addition to the way privacy laws apply in the "real" world, there are some special things to think about when dealing with the Internet and e-business.

Privacy Policies on Websites

You should fully understand how your website fits into privacy law requirements.

- If your website collects personal information, whether by asking for names, phone numbers, e-mail addresses, mailing addresses, etc., you should develop a proper and legally compliant privacy policy and post in a readily visible location on your website.
- If you use cookies or similar means to track visitors, depending on how you do that, you may still need to develop and post a policy.
- Online profiling may require the consent of the individual depending on the circumstances.

Keep in mind that people do look for privacy policies so, without a policy, you may lose prospective customers. A properly drafted privacy policy or statement will not only minimize your legal exposure, it can serve a marketing function as well, allowing you to attract and retain customers who otherwise might not be as inclined to deal with you.

Whatever you do, do not create a policy and then not follow it precisely. This is an invitation for disaster, including not only possible legal problems, but also injury to your reputation and goodwill.

It is therefore important to not just let the policy sit once it has been posted. It should be revisited regularly to determine whether or not it is still accurate and to evaluate whether or not it should be revised to assist you in your business goals and objectives.

Platform for Privacy Preferences (P3P)

Lastly, keep in mind other privacy or related technical issues that may cost you customers and money. For example, P3P, or the Platform for Privacy Preferences, now allows websites to encode their privacy practices in a manner that some browsers, such as recent versions of Internet Explorer, can "read." So, if a visitor to your site has configured their browser to reject your type of configuration, they may receive error or time-out messages. They may not be aware as to why they can no longer log in, and you may not be aware that you've lost them.

Summary

Privacy laws may sound confusing at first, but much of it is common sense. By understanding the fair information principles, you will be better prepared to develop a proper privacy policy. Moreover, if you obtain proper legal advice, your online business should proceed with minimal difficulties.

Resources

- Canadian Bankers Association – Minding Your E-Business
  www.cba.ca/en/section.asp?fl=3&sl=89&tl=247&docid=
- ebiz.enable – Privacy Section
  http://strategis.ic.gc.ca/epic/internet/inee-ef.nsf/en/h_ee00237e.html
- EU Data Protection Directive
  www2.echo.lu/legal/en/dataprot/directiv/directiv.html
- Office of the Information and Privacy Commissioner of Alberta
  www.oipc.ab.ca
- Online Privacy Alliance
  www.privacyalliance.org
- Organization for Economic Cooperation and Development
  www.oecd.org
- Privacy.org
  www.privacy.org
- Privacy Commissioner of Canada
  www.privcom.gc.ca

Contact Us

The Alberta E-Future Centre, a service initiative of The Business Link, is your first stop for e-business information in Alberta. We offer free, impartial, and easy-to-understand e-business advice and information for small and medium-sized businesses. Our goal is to help entrepreneurs make more informed decisions as they adapt to technological change. If you have any questions, we are only a visit, click or a call away!

Alberta E-Future Centre
The Business Link Business Service Centre
100 -10237 104 Street NW
Edmonton, Alberta T5J 1B1
Tel: 1-800-272-9675
Fax: 780-422-0055
E-mail: alberta@e-future.ca
Web: www.e-future.ca/alberta

This guide was prepared by the Alberta E-Future Centre
www.e-future.ca/alberta

A member of the Pan-Western E-Business Team