

This article appeared in the May 2004 edition of eLondon Magazine. It is reproduced with permission.

Copyright 2004. All rights reserved

Everything you wanted to know about privacy compliance but were afraid to ask David Canton

All organizations must comply with the new privacy laws that came into effect on January 1, 2004. This article outlines the new laws and how businesses should approach becoming compliant. It is not as daunting a task as it might first seem.

The privacy concept

Privacy is the right of an individual to determine when, how, and to what extent they will share personal information about themselves.

Personal information is any information about an identifiable individual. It includes such things as banking information, buying habits, health information, address, location, and so on. The Supreme Court of Canada says that, "this notion of privacy (of information) derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain as he sees fit." In other words, each individual has the right to determine what others can do with information about them.

The recent emphasis on privacy is not merely a Canadian phenomenon. Privacy legislation in Europe predates that of North America. In the United States, privacy legislation has been enacted in various business sectors, including financial services and health.

Laws relating to privacy are not limited to businesses selling goods over the Internet, they apply no matter what the nature of the business or how the information is stored. The only relevant factor is whether the organization deals with information about individuals. It should be noted that privacy laws generally do not apply to information about corporations.

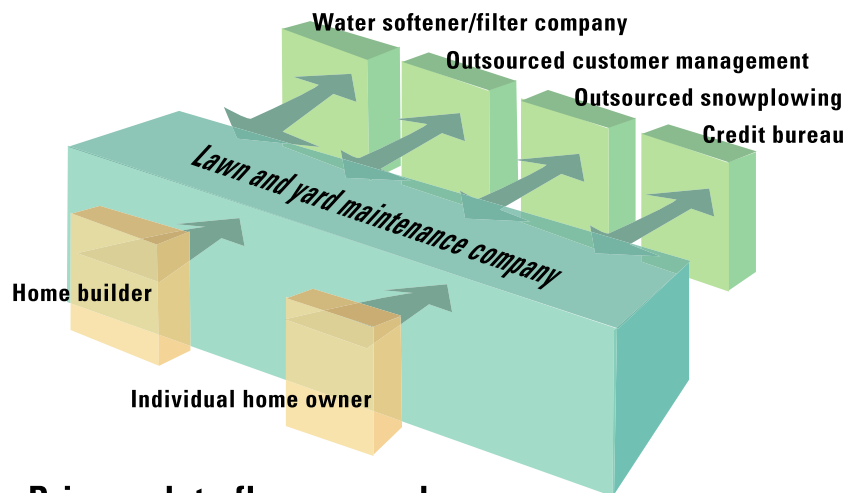
Advances in Internet and ubiquitous computing have, in part, driven this recent interest in privacy. It is easier now, than ever before, to collect, combine, manipulate and disseminate information about individuals.

Applicable laws

Canada has had privacy legislation affecting governments and government bodies for some 20 years. These laws include the Federal Privacy Act and the Ontario Freedom of Information and Protection of Privacy Act. The Federal Personal Information Protection and Electronic Documents Act (PIPEDA) has been in effect for more than three years for federally regulated businesses, such as banks and airlines. PIPEDA applies to all provincially regulated organizations as of January 1, 2004 unless a province enacts similar legislation in the meantime.

Ontario has not yet passed its own privacy legislation, though it is expected to do so in the future. A draft act was proposed some time ago, but did not make it past the draft stage.

Ontario has tabled the first reading of the Health Information Protection Act. This legislation is intended to apply to the health sector and will encompass doctors, hospitals and other healthcare services. The definition of healthcare in the draft includes any "...observation, examination, assessment, care, service or procedure that is done for a health related purpose



Privacy data flow example

Personal information in the case of a lawn and yard maintenance company might include customer identity, address, financial and credit information, family details, time of day/year when house is unoccupied. Issues include consent to send information to water softener company; consents of home builder and water softener company to provide information; maintenance staff should not see financial information; flowing through obligations to third party service providers; security of data.

Copyright 2003 © Harrison Pensa LLP All rights reserved.

and that...is provided to prevent disease or injury or to promote health..." This definition is very broad and could apply to many businesses that might not expect it to, such as fitness clubs.

The final form of the Health Information Protection Act or an eventual Ontario general privacy act is not yet known. The general privacy act is expected to cast a broader net than PIPEDA and capture non-commercial uses and the employer/employee relationship, neither of which are covered by PIPEDA.

Businesses should not feel that current compliance with PIPEDA is a waste of time or that it is money that will lead to duplication when provincial legislation is in force. The process for compliance will be similar, and the groundwork and diligence efforts for PIPEDA will not have to be repeated for provincial legislation. While some details may differ, the basic privacy principles will be the same.

Many businesses are implementing employee privacy policies even though it is not necessary as they feel it is the right thing to do. Many charities are also complying, even though they do not need to do so provided they do not engage in "commercial activities" such as selling donor lists.

PIPEDA obligations

PIPEDA adopts the CSA model code, which contains ten privacy principles:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

These ten principles set out the ground rules for how organizations may collect, use, and disclose personal information in the course of commercial activities.

Businesses must appoint someone (or more than one person), commonly known as a privacy officer, to be accountable for their privacy policies, and to publish these policies.

The fundamental requirement is that consent must be obtained from individuals for the collection, use, or disclosure of their personal information.

At the time of collection, a business must identify the purposes for which the information will be used. For example, purporting to collect information for a survey—then later trying to sell a product to that person based on the answers to the survey—would be a violation of this principle.

Consent must be obtained from the individual to collect, use, and disclose their personal information. Implied consent is acceptable under certain circumstances but should not be heavily relied upon. For example, if one subscribes to eLondon magazine, it would be reasonable to expect eLondon to use the subscriber's address information to send the magazine, to send a renewal notice when a subscription lapses, and to collect subscription fees. It would not, however, be reasonable to expect eLondon magazine to provide that name and address to an Internet service provider to enable them to sell their products to the subscriber. Such a use would require a specific consent—which is why you often see check-off boxes on subscription cards asking if they can provide your name to others.

Businesses are not to collect information that is unnecessary for the described purposes. For example, a subscriber to eLondon magazine should not be expected to disclose their date of birth. The use, disclosure, and retention of information must be similarly limited to the extent necessary to fulfill the described purpose.

The legislation requires security measures to be in place that are commensurate with the sensitivity of the data. In other words, security safeguards must be more robust for sensitive information, such as banking and health information, than for address information. Security requirements must be looked at in light of the way the organization deals with the data. Such measures might include everything from locked filing cabinets and restricted access to offices, to sophisticated access controls and encryption on their computer networks. Keep in mind that privacy and security is not the same thing. A bird in a cage is secure, but it is not private.

Individuals are entitled to obtain access to all of the information a business has about them.

So what if a business does not comply with PIPEDA?

PIPEDA contains fines of up to \$100,000 for obstruction of an investigation, disciplining a whistle blower, or destroying information after it has been requested.

Anyone may complain to the Privacy Commissioner if they feel an organization has violated privacy principles. The Privacy Commissioner is bound to investigate unless she feels that the complaint is frivolous. Such an investigation can be costly and time-consuming for a business.

If the Privacy Commissioner issues its report and finds that the organization has breached the legislation, and the organization does not correct its behavior, either the complaining party or the Privacy Commissioner can take the matter to court. The court has the power to issue orders to comply, to force the business to publish corrective action in the press, and to award damages.

“

By the end of the decade, much of entertainment and media content will be in a digital format. Yet, while new products and services generated by digital technology are driving market growth, digitalization also creates almost **unlimited opportunities for unauthorized usage.**”

OLIVER WOLF
PricewaterhouseCoopers

Steps to compliance

PIPEDA has been widely criticized as being difficult to understand, and difficult to apply in practice, especially for small businesses. That should not however dissuade a business from doing its best to comply with the legislation.

Compliance is more than simply copying someone else's privacy policy from the Internet. Each business's policy must be tailored to its own needs. A common mistake is to draft the privacy policy too tightly and unduly restrict the business.

There is a process that each business should follow to become compliant. A more detailed privacy compliance checklist can be found on the Harrison Pensa website (www.harrisonpensa.com).

The first step is to appoint a privacy officer. This person should be senior enough to wield some influence within the organization and should have an interest in privacy matters.

The next step is to perform a privacy audit or privacy diligence. The privacy officer should talk to people within various areas of the business to determine:

- How each area collects and uses personal information
- The flow of that information to determine how it is used within the organization and to what third parties it is sent
- How uses of information are explained to the individual and consents are obtained
- How the information is stored and what security is in place (don't forget things like backup processes and the disposal of old storage media and equipment)
- How information is disposed of when it is no longer required (for example, are paper documents shredded rather than put in the trash?)

It is important to consider every facet of a business that touches personal information in any way, what it

does with it, and what opportunities there are for the information to get into the wrong hands.

After the audit has been performed, the business will be in a position to compare their results to the PIPEDA requirements to determine what, if any, changes need to be implemented regarding its processes and documentation. The organization should draft a privacy policy that reflects PIPEDA privacy principles and the practical business requirements of that organization.

The next step is to publish the privacy policy and train employees about their privacy obligations.

Legal assistance should be sought before starting the diligence process, to assist in comparing the audit results to PIPEDA requirements, and to draft a policy.

But my business deals with other businesses—not individuals

A business should not simply decide that it does not need to comply with privacy regulations simply because it does not deal with individuals without first conducting a high level privacy audit. Even a business that has only other businesses as customers may deal with unincorporated businesses, which are considered individuals and thus subject to PIPEDA. The business may also have information on individuals within other companies, such as personal details about its sales or purchasing staff.

A business that provides services to other businesses—such as data processing—may not collect information about, or deal directly with individuals, but may in fact deal with very sensitive information about their customers' customers. A business is obligated under PIPEDA to obtain certain privacy assurances from third parties to whom it provides information. Indeed, a business is still responsible under PIPEDA if a subcontractor misuses personal information.

Service providers should take a proactive approach and create a privacy policy and privacy language for its contracts. For example, it might include in its service contracts that it will not use information provided by their customer for any use other than that contracted for by the customer, that it will keep the information secure, and that if it subcontracts any portion of the responsibilities, it will flow these privacy obligations through to the subcontractor.

Even though a service provider business may not interact with individuals directly, it is still responsible for the other aspects of PIPEDA, such as security and restrictions on the use and disclosure of that information.

Digital toys

We all want to have the latest digital toys, but we must keep in mind that they are especially susceptible to privacy violations.

Data enabled cell phones and PDAs let us stay connected and perform our jobs away from our desks and outside the office. In doing so, these devices contain data such as contact information, customer information, financial information, and virtually any information that one might have on their systems at work.

All the efforts to secure a corporate system will not prevent the information from being disclosed if a cell phone or PDA is lost. Consideration should be given to password protection or encryption on portable devices if it might contain sensitive information.

Case studies: three London businesses that have become PIPEDA compliant

PROTEK SYSTEMS

Protek Systems provides computer systems and technology related services. Harvey Schilke, Protek Systems' President, initially thought PIPEDA compliance was simply another government make-work project. However, Protek found the process a valuable experience. It enabled them to better understand their own privacy issues and those of their customers. It made them aware that PIPEDA is a good reason for their customers to review their IT security to ensure privacy compliance. Protek learned that privacy issues impact the company and its customers. Protek looked seriously at the technology they were providing to their customers to ensure it was compatible with privacy concepts. Schilke sums it up by saying that Protek now "takes it seriously enough that its privacy officer is one of the owners of the Company."

LONDON HYDRO

Nancy Hutton of London Hydro says that the process of developing and implementing a privacy policy was a positive experience. It provided:

- an opportunity to review personal information collected throughout the organization
- confirmation that their existing procedures already had the interest of their customer's privacy as a priority
- an opportunity to streamline a few of their existing procedures

The process left London Hydro confident that their policy meets the requirements of the new privacy legislation.

TLS

Davyd Funk, Vice President of TLS, says that being in the out sourced call centre business, gathering personal information is something that happens at TLS thousands of times a day. This is always on behalf of another business, and these businesses look to TLS to be at the forefront of knowledge on how to collect information as well as the rules and regulations concerning that collection so they act responsibly. Implementing a policy that met its specific business situation was definitely the way for TLS to be compliant. Funk also comments that, in his view, the steps to compliance have been logical and conform to common principles of courtesy and respect for personal privacy. "At no time have I felt that this was really changing the way we do business, rather it has sharpened our focus on being responsible in terms of the way we do business with individual consumers. Thinking of personal information as data that is on loan for the purpose of providing a service rather than a commodity has been the way I have tried to educate my business customers—they get that quite readily." Over the long term, being conscious of the implications PIPEDA has brought forward is good for business and for TLS. The consumer that unconditionally gives out their information is a fading breed. Today's consumer expects an exclusive relationship with clear terms. PIPEDA ensures this, and by being a compliant company, TLS helps business customers meet that need. Funk recommends that businesses become compliant sooner rather than later. "I feel the consumer has been there for a while already, certainly when I think of myself I do not fill out subscriptions without reading the fine print and checking the do not mail me things box."

Goodwill's



**TEMPORARY
STAFFING**
source

Serving London and surrounding areas

EMPLOYER HOTLINE

850-8367

379 Dundas St., London Towers, Suite 19
temporarystaffing@londongoodwill.on.ca

www.gtss.ca

We believe in the power of work!

general labour • clerical • data entry
warehousing • assembly • collating
flyer delivery • janitorial • cleaning
residential yard work • moving
• and much, much more !

Privacy affects the value of your business

Privacy is becoming a real concern in the area of business acquisitions. When purchasing a business, it will become increasingly common for the purchaser to perform privacy due diligence in addition to the traditional diligence process. Depending on the nature of the business, this could include investigations into the business's privacy policies and practices and obtaining privacy related warranties from the business.

If one of the assets of the business being purchased is customer information, it is important for the acquiring business to know whether privacy rules allow that information to be transferred to it and, if so, how it must be accomplished. Depending on the business's privacy policy, the transfer and use of customer information may not be available to the purchaser without costly steps.

Thus, not having your privacy house in order can reduce the value of your business. No one wants to purchase a business that has a lackadaisical attitude toward privacy, as it may be buying all that business's privacy problems and complaints.

“

Don't do anything with anyone else's information that you would not be comfortable having someone else do with yours. ”

Final thoughts

Businesses need to deal with privacy because it is now the law. Given that the law is in place, businesses should approach privacy with the attitude that they will use it to its advantage.

Compliance with privacy legislation has many advantages, including:

- Avoiding damages to the Company's reputation, particularly "headline risk" in the press
- Avoiding civil and class-action lawsuits that may result from abuses of personal data or unfair or deceptive information practices
- Showing your customers that you take privacy seriously
- Enabling a company to do business in other countries having their own privacy laws
- Obtaining the trust of your customers so they won't give false information
- Obtaining a competitive edge over competitors who have failed to embrace privacy

Over the next few years, privacy obligations will become clearer as the courts interpret the legislation, privacy commissioner decisions are rendered, and the court of public opinion determines what is expected. For now, businesses should do their best to comply with the spirit of the legislation and do the right thing regarding privacy.

Adopt the Golden Privacy Rule: don't do anything with anyone else's information that you would not be comfortable having someone else do with yours. ■