Privacy and your clients

An agenda for every firm

When lawyers think of privacy compliance, many probably think about advising business clients about the requirements of the federal ***Personal Information Protection and Electronic Documents Act*** *(PIPEDA). This statute, which will apply to all businesses on January 1, 2004, requires all Canadian businesses to implement policies and procedures to safeguard personal information. What lawyers may not fully recognize, is that they too are businesses – and they too must act to protect personal privacy.*

By Simon Chester, Partner
McMillan Binch LLP

al Indemnity Company. This rticle originally appeared in LAWPRO
g Your Practice Soar", Sur er 2003. It is available at
www.lawpro.ca/magazin rchives

Where is this coming from?

PIPEDA has applied to federally regulated employers for almost three years now. It sets out rules for the collection, use and disclosure of "personal information" about customers, clients and employees in the course of commercial activities.

Effective January 1, 2004, Ontario businesses will also become subject to the requirements imposed by PIPEDA, until any "substantially similar" provincial legislation is proclaimed in force. In 2002, Ontario circulated a draft privacy bill for consultation purposes. All indications point to provincial legislation being shelved until after the Ontario election – or perhaps indefinitely. Whatever the source of privacy obligations, the standards are going to be substantially similar to PIPEDA – and law firms are going to have to comply.

What is "personal information"

The statute cuts a broad definition. Personal information includes any factual information about an "identifiable individual," recorded or not, and includes age, identification numbers, income, ethnic origin, employee files, evaluations, credit and loan records, and medical records. Personal information does not include an employee's name, title, business address or phone number. An e-mail address seems to be personal information.

What is required to protect personal information

PIPEDA's requirements stem from 10 basic principles, developed by the Canadian Standards Association, which are explicitly set out in the legislation. These principles articulate guidelines for what businesses must do when they collect, store and use or disclose confidential information. (See **The 10 principles of privacy** on page 16 for a brief explanation of each of these principles.)

What will PIPEDA require law firms to do?

First, every law firm will have to formalize its privacy practices and procedures. This will mean systematically examining their practices and how they use personal information. Not all practices are the same, since difference practice areas handle greater or lesser amounts of personal information. Criminal defence lawyers' offices are likely full of extremely confidential personal information. A small firm which deals in family law or estates matters, or whose clients are largely individuals, is more likely to have sensitive information in its files than a large business firm whose clients are corporations.

Coping with the new law

A number of Ontario firms have already taken steps to comply with the new law. For Merv White of Orangeville's Carter and Associates, the firm's privacy policy sprang out of work he was doing to advise the firm's many charitable and not-for-profit clients. He drafted a Privacy Policy which can be found on Carter and Associates' Web site (www.carters.ca/privacy.pdf), as well as a detailed internal Policy Implementation Manual. His advice to his colleagues in other firms – "you'd better get your privacy policy in place – this issue is not going away."

Gowlings is an Ontario firm that ranks as one of the largest in the country. Michael Power of Gowlings' Ottawa office drafted its policy initially. Because the firm maintains offices in Vancouver and Calgary, it will face a complex implementation task, taking account of new bills introduced in the western provinces.

Mr. Power's draft went through a round of "peer review" by colleagues and then went to the firm's executive committee. The most controversial issue was how privacy obligations matched up against professional responsibilities. Gowlings explains carefully to the clients and potential clients the concept of solicitor-client privilege and when it arises within a professional relationship.

Powers predicts that the new rules will not dramatically affect his firm – "we deal in information so we're likely to have an easier time adjusting." It would affect any firm that engages in "shotgun" marketing techniques as you will need consent to market in this way.

What does your firm need to do now: A compliance checklist

Building on the 10 principles, the following checklist will help you sort through the steps you need to take to comply.

- **Read the Personal Information Protection and Electronic Documents Act.** Understand privacy law and how the privacy principles impact your firm. The Web sites of the Privacy Commissioner of Canada – www.privcom.gc.ca – and of the Information and Privacy Commissioner of Ontario – www.ipc.on.ca – provide good starting points for both you and your clients.
- **Select a privacy officer.** Pick a firm member who can assume responsibility for privacy. Give this privacy officer the resources needed to meet the new requirements.
- **Look at your practice.** Assess the impact of the privacy principles on your clients. Not all firms will be affected in the same way.
- **Develop a privacy policy.** Your new privacy officer should work over the next year to set policies and procedures for protecting privacy and addressing complaints, train staff to adhere to the privacy policies and procedures, and develop your public positions on privacy.
- **Track data flow.** Identify your personal information holdings. Track how personal information is collected. What sensitive information do you have on clients or third parties? How is it circulated internally? What is personal information used for? Is it ever sent outside your business? You need to map data flow within your business to identify vulnerabilities. Rationalize your personal information handling practices.

- **Revise your contracts.** The new law will require that privacy is protected when data leaves your firm. In your agreements, you must ensure that the other parties (e.g. process servers, title searchers, investigators, experts) who receive or process personal information provide the same protection that you do, and will not disclose this information to others.
- **Ensure consent.** Do you ask for consent when you collect information? You should review all your consent provisions to ensure they meet the new law. Make consent meaningful. The form and manner of consent that is required will depend on the sensitivity of the information and the surrounding circumstances.
- **Security systems.** Computer security is very important. Make sure personal information is secure, by keeping it physically and, where applicable, electronically protected. Design or change existing information management systems. Check firewalls of your computer system for vulnerability. Test and evaluate systems and processes.
- **Support staff training.** Your assistant or secretary has a key role to play in ensuring that personal information is kept truly confidential. Train your legal support staff on the changes you are implementing.
- **Allow access.** Establish procedures to allow individuals access to their personal information, and to correct or update information when appropriate.
- **Finally, educate your clients and help to inform the public.** The obligations are going to fall on every business or other entity in the province engaged in commercial activities. They are going to need help to understand a broad-ranging and unusual statute that speaks in terms of principles rather than specific statutory requirements.

Model privacy policy for law firms

LawPRO has a generic policy, which you can use as a precedent and checklist to guide you as you examine your own firm's procedures for dealing with confidential information. The policy deals with a fictitious firm called Smith & Partners. It is available at www.practicepro.ca/privacypolicy.

What are the risks of non-compliance?

A failure to comply can expose your firm to a number of costly, time-consuming and potentially embarrassing circumstances. PIPEDA makes the federal Privacy Commissioner responsible for ensuring compliance with the Act and for promoting its purposes. The Commissioner has five main ways of ensuring that organizations subject to the Act adhere to its principles:

- investigating complaints;
- mediating and conciliating complaints;
- auditing personal information management practices;
- publicly reporting abuses; and/or
- seeking remedies in court.

An individual may complain to the organization in question or to the Privacy Commissioner about any alleged breaches of the law. The Privacy Commissioner may also initiate a complaint. This will prompt an investigation and the preparation of a report.

After receiving the Commissioner's investigation report, a complainant may, under certain conditions, apply to the Federal Court for a hearing. The Privacy Commissioner may also apply to the Court on his own or on the complainant's behalf. The Court may order an organization to change its practices and/or award damages to a complainant, including damages for humiliation suffered.

The Privacy Commissioner may, with reasonable grounds, audit the personal information management practices of an organization.

An audit or complaint that results in a public report about breaches of compliance at your firm would be very embarrassing.

Anyone who believes that any of Sections 5 to 10 of PIPEDA have been or are about to be contravened, may notify the Privacy Commissioner, and ask that his or her identity be kept confidential. Once the Privacy Commissioner has given his assurance, he is bound to protect the person's identity.

It is an offence to:

- destroy personal information that an individual has requested;
- retaliate against an employee who has complained to the Privacy Commissioner, or who refuses to contravene Sections 5 to 10 of PIPEDA;
- obstruct a complaint investigation or an audit by the Privacy Commissioner or his delegate.

A person is liable to a fine of up to $10,000 on summary conviction or up to $100,000 for an indictable offence.

Employees

For constitutional reasons, the federal law stops short of imposing privacy obligations on workplaces. It grants privacy rights only to employees in federally regulated workplaces. Until Ontario passes its own privacy legislation, there are no mandatory requirements. Nevertheless, given an increasingly privacy-conscious public, your employees may wonder whether their personal information is being adequately protected.

As with other personal information, you will need to ensure that your personnel files are both physically and electronically secure. You will also need to safeguard health information about your employees, and protect the identity of those who take advantage of employee assistance programs.

Ensure that your employees understand the importance of privacy. Develop clear written policies for your employees about how you, as their employer, treat privacy issues.

Michael Powers of Gowlings adds "firms with offices in BC, Alberta and Quebec will have to address the subject of employee privacy. This will impact student as well as employee evaluations (since people will have access rights)." Firms are going to have to be more careful on hiring practices and employee evaluations.

Next steps

For most law firms, complying with privacy law should not impose a significant burden. It's going to require some attention over the next six months, but once your policy and systems are in place, you'll largely be responding to any inquires and making sure that your firm is living up to its commitments. As Ontario's Information and Privacy Commissioner, Dr. Ann Cavoukian tells businesses "the fact is that good privacy is good business – it fosters trust, builds consumer confidence, strengthens brand recognition, increases customer loyalty and ultimately delivers competitive advantage."

For lawyers, a final point is that protecting privacy aligns with our professional obligations to preserve confidentiality. By January 1, 2004, it will also be a legal requirement.

The 10 principles of privacy

The following 10 principles provide an overview of what businesses must do when they collect, store and use or disclose confidential information. For the full text of the principles see www.privcom.gc.ca.

#1 Accountability – An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the legislation's privacy principles.

#2 Identifying Purposes – The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

#3 Consent – The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

#4 Limiting Collection – The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

#5 Limiting Use, Disclosure, and Retention – Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

#6 Accuracy – Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

#7 Safeguards – Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

#8 Openness – An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

#9 Individual Access – Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

#10 Challenging Compliance – An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.