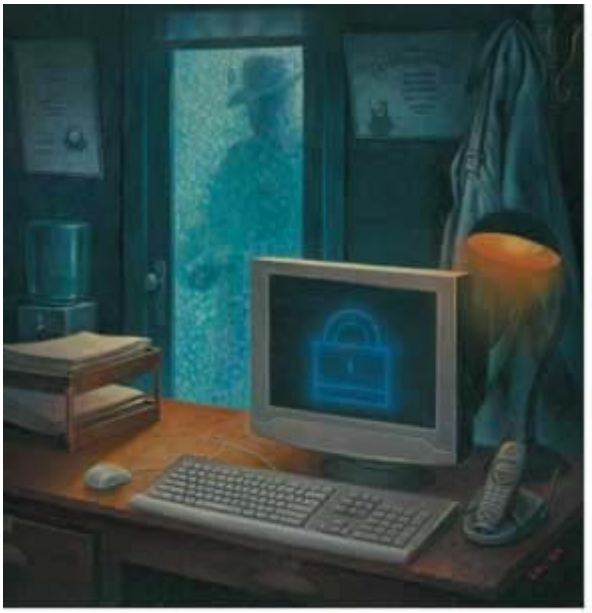
STRENGTH BEYOND NUMBERS
camagazine.com

Privacy rules

By Erin R.Kuzz & Rob Colapinto
Illustration: Joe Salina



IN JANUARY, THE ACT GOVERNING PERSONAL INFORMATION WILL COVER EVERYBODY. ARE CAS PREPARED? DO THEY HAVE THE RIGHT PRACTICES TO BE COMPLIANT?

It was certainly the most original and revealing flyer in Toronto's booming real estate market, a real eye-catcher. The front page was not unusual — it flogged some of the city's finest homes — but if any of the thousands of recipients had flipped it over, they would have discovered details of an Ottawa woman's medical history and recent mammogram. Somehow this record had made a conspicuous detour after she asked that her file be forwarded from her doctor to her lawyer. At some point, it made its way to a recycling bin and on to a printing company. The privacy and security of highly personal information had been breached in the most public of ways.

"That's the true nightmare scenario for businesses large and small," says Peter Sievers, a partner with Calgary-based Expatriate.Com, a consulting firm specializing in expediting the tax needs of Canadians relocating abroad. "You just have to shake your head, especially in this time of heightened public concern over privacy." As he speaks, Sievers makes a note to double-check the procedures of the mobile document shredding company that destroys his most sensitive client files. "Accountants, I expect, should nearly top the list when it comes to appreciating the importance of privacy."

Indeed, CAs and lawyers stand at the forefront of a soon to be hot specialty: privacy management and compliance. Because of the important advice-giving role played by accountants and lawyers, these professions will need to be ahead of the curve in terms of understanding and advising clients of their privacy obligations. Failure to do so could prove costly and embarrassing for all parties. CAs need to ask if their offices have sufficient privacy practices in place to avoid costly errors. Given the volume of personal information CA firms hold on client files, do they have appropriate retention and destruction policies that are actually followed by employees? It's time to check.

The misuse of personal information has been a looming spectre for business since the computer's transformation from a benign information storage curio to the principal tool for collecting, tracking and interpreting data for the global economy. But only in the past few years have formal legislative measures been taken to provide some control over the collection, dissemination and security of personal data.

Privacy concerns had been developing in Europe since the early 1970s as a result of

growing information databases and the use of personal identifiers to tag personal information. Sweden was the first country to pass a data protection act in 1973, soon followed by Germany, Denmark, Norway and France. In 1995 the European Union issued a directive to its member states requiring them to bring their national data protection laws into compliance.

Since the early 1980s Canadians have enjoyed legislated protection regarding personal information used by municipal, provincial and federal governments. In 1996 the Canadian Standards Association developed a voluntary privacy code based on the OECD privacy guidelines. It included the concepts that individuals have the right to know what personal information about them is being collected, used and disclosed; the right to know who is collecting personal information and for what purpose; the right to reasonably limit the collection, use and disclosure of personal information through the exercise of consent (in most cases); the right to access personal information to ensure its correctness and challenge legal compliance. It also made organizations responsible for the information they gathered and used, and required they be open with their information management practices.

In 2001 the federal Parliament enacted Canada's first set of commercial privacy standards, the Personal Information Protection and Electronic Documents Act (PIPEDA). The law, which affects only government institutions and federally regulated companies, has broad reaching implications and seeks to balance the right of the individual to privacy with the need of organizations to collect, use and disclose personal information in the course of commercial activity.

On January 1, 2004 PIPEDA will move into full gear, requiring privacy compliance from all private-sector commercial activity. From mom-and-pop storefronts to Canadian-based conglomerates, the concept of privacy as a legal issue will have to be addressed. For some organizations, attaining privacy law compliance will be daunting and costly. For others, it will entail a relatively straightforward audit and compliance program. Either way, for most organizations, the potential cost of non-compliance is simply too high.

PIPEDA is similar to the CSA's privacy code, but where the latter is voluntary, the former requires by law that organizations, among other things, designate an individual or individuals who will be accountable for the organization's compliance with PIPEDA, and seek appropriate consent for the collection, use or disclosure of personal information. Indeed, the legal concept of consent is a fundamental element of PIPEDA; it may be either express or implied. However, whenever possible, organizations should protect themselves by obtaining informed and express consent. This requires an organization to clearly set out the purpose for which the information is being collected, used and/or disclosed and to ensure individuals understand and appreciate these purposes, which themselves must be "reasonable." Organizations must also obtain fresh consent whenever the use for which the information was collected has changed.

Consent is not required if a court or administrative tribunal orders disclosure of personal information; if the personal information is collected during an investigation into a violation of an agreement (such as an employment contract) or contravention of a law; if personal health information is disclosed in an emergency that threatens the life or health of the individual; and if collection is clearly in the interest of the individual and consent cannot be obtained in a timely way (although these exceptions are likely to be very narrowly interpreted by Canada's privacy commissioner, courts and arbitrators).

Every organization in provinces without legislation substantially similar to PIPEDA will be governed by it, and the government of Canada will decide if the legislation is similar. If the provincial legislation is substantially similar to some portions of PIPEDA, the province will be governed by both federal and provincial legislation. Quebec already has substantially similar privacy legislation, whereas Alberta and British Columbia have introduced privacy legislation.

“To me [PIPEDA] is good for the business world,” says Robert Parker, partner at Deloitte & Touche responsible for personal information privacy within Canada. Parker has spent much of the past 10 years involved in privacy issues. PIPEDA, he explains, offers business clear guidelines for obtaining proper consent to use personal information. “When [a business] looks at privacy it should say: what is it we want to accomplish? Do we want to create customer goodwill, maybe increase brand recognition?” he says. “Well, you go about these things by using privacy as a driver for commercial activity.”

PIPEDA has created fertile ground for CAs and lawyers investing in specialized privacy practices. PIPEDA’s measured approach to compliance and information access offers a twofold opportunity: the service of the CA as a compliance auditor and working with lawyers as part of a team of consulting professionals on how best to meet privacy law requirements.

“What the CA is particularly well-suited for is verifying or auditing whether a company is complying with the legislation,” says David McKendry, former director of Price Waterhouse’s privacy consulting practice. “As well, CAs understand systems and understand business procedures and strategies. That’s pretty well what privacy is all about.” McKendry is a sole practitioner and a former CRTC commissioner and chair of the committee that created the CSA’s voluntary privacy code. He currently specializes in privacy and regulatory issues, focusing on the actual implementation of PIPEDA’s main principles. “Just knowing them is not enough,” he explains. “It requires specialized knowledge and companies will have to have people who understand the scope of the act and its meaning and interpretation.”

Unfortunately, few CAs and their firms have the expertise garnered from McKendry’s decade-long focus on privacy issues. Most, according to the CICA and the American Institute of Certified Public Accountants, have yet to get their own compliancy houses in order. Paul-Emile Roy, a principal with the CICA’s research studies, is less than confident the profession is prepared for the onslaught of PIPEDA-related queries from their clients.

On a preparedness scale of one to 10 — with the exception of the large CA firms, which have made a point of educating themselves and their clients — most accountants are at a one, he says. “They have little or no appreciation of PIPEDA or any other privacy related obligations.”

Parker laughs at his friend’s grim assertion, but agrees: “Many businesses and professionals have yet to fully address the privacy legislation requirement.”

To help CAs comply with the new laws, the CICA has put together a privacy package with all the relevant information. It can be accessed at www.cica.ca/privacy.

Sievers — perhaps because he is in the throes of updating the website complementing his growing practice — is determined to get it right from the get-go. “With an online service, ignorance of any law or code related to privacy and security would be the kiss of death,” he says. The Internet, of course, has been the lightning rod for privacy complaints and consumer mistrust since it came online and quickly established itself as a key purveyor of personal information.

Although Sievers is less than confident that any legislation will allay public suspicion online — “the Internet is interconnected globally, and I wonder about the safety of my personal data once it passes beyond PIPEDA’s reach.” He is taking every step to be in compliance. He is well aware that if egregious brick-and-mortar gaffes on the scale of the revelatory real estate flyer were perpetrated on the Internet, he would be finished. “This kind of breach is magnified a thousandfold when it’s sourced from the Internet. We’d simply have to close up shop,” he says.

A recent Harris Interactive poll for the Privacy and American Business Study confirms the growing public intolerance for privacy violations. It found even if customers had no intention

of revealing personal information to a business, 83% would take their business elsewhere if it were found to have improperly used personal information. On the Internet, where this suspicion is rife, such an overwhelming sentiment does not bode well.

“The protection of privacy is ultimately a control issue,” says McKendry, “and by that I mean the ability of the individual to control the collection and use of personal information.” Ideally, PIPEDA will provide the individual with these controls. It will also control the parameters within which businesses will be allowed to use information legally and as a business tool. For Internet e-commerce, McKendry believes it will be up to business to have the first go at changing its mind-set, its way of thinking about how privacy is used. Only then can it reasonably expect to garner renewed confidence from consumers. If business views privacy legislation as an impediment to both online and offline commercial activity, it will have constructed an unnecessary barrier to effective commerce. “Corporations need to acknowledge and recognize that individuals now have the ability to control the use of their personal information,” he says. To deny them that right will not only be bad for day-to-day business but it is also illegal.

So who is responsible for supervising the application of the legislation? The Privacy Commissioner of Canada (PCC) is the officer of Parliament charged with overseeing privacy legislation in the federal sphere and does not report to any single minister. The commissioner’s powers are broad and include the power to audit any organization when there are reasonable grounds to believe that there is an issue of non-compliance. In the process of conducting an audit, the PCC can summons a person to appear and give evidence; the PCC can also enter a commercial building to speak to anyone or gather documents. After an audit, the PCC is required to provide the organization audited with the results of the audit as well as appropriate recommendations.

The PCC also has authority to investigate any third-party complaints with evidence-gathering powers and reporting obligations like that of an audit. In some circumstances, a complainant can request that the PCC’s findings be reviewed by the Federal Court, which has the authority to grant any remedy within its jurisdiction. This can include an order that the organization comply with PIPEDA, and/or pay monetary damages. If the organization is facing complaints from several people, this could mean considerable liability.

The PCC, however, does not have the power to issue a fine or file a criminal or quasi-criminal charge for non-compliance with the act (although courts do in certain circumstances). The PCC attempts to use mediation and persuasion to resolve complaints and ultimately has the power to determine whether a complaint warrants further investigation.

This lack of formal legal enforcement power doesn’t mean that the PCC is without the ability to punish organizations in violation of PIPEDA. One way the PCC can do this is to make public the name of an offending organization if such a revelation is in the public interest. The PCC may also disclose to the attorney general of Canada or to any province information about the violation of any law even if that information is unrelated to privacy issues. Bad publicity, says Parker, is the most effective deterrent. “A US study, The Privacy Blow-Out,” he recalls, “found that repairing a small business’ reputation would cost about $50,000, and for large firms it’s about $1 million.” For Internet companies, recovery from such a public flogging could almost be impossible.

Obviously it is important to comply with privacy law for legal reasons, but doing this for only that reason fails to recognize the benefits compliance can bring to an organization. Effective privacy compliance is currently a necessary part of doing business and staying competitive. It is fundamental to obtaining and retaining accurate customer and employee information, customer and employee trust and loyalty, international business opportunities and ultimately, profit.

Organizations can be devastated if the PCC publicly names them as offenders. For

example, some organizations seeking to be privacy-compliant have refused to do business with organizations that are not compliant out of concern that personal information ordinarily exchanged during the course of business will not be properly protected.

As well, customer and employee mistrust can result in the withholding of personal information that would otherwise be necessary for efficient business practices and product development.

The benefits of protecting privacy are thus more obvious when organizations understand how existing or potential customers, business partners and employees value privacy, as well as the potential costs of a privacy breach in terms of reputation and the bottom line.

Some companies such as Indigo-Books & Music Inc., which includes Chapters Online website, have long understood the importance of privacy compliance. Deirdre Horgan, vice-president of marketing, says the company had seen formal legislation coming down the pipeline long before the online business was launched in 1998. “We’ve worked as though it was already ironclad and very, very strict,” she says. The company has used the privacy issue as a positive support for its commercial activity. Its privacy charter is clear and unambiguous: the customer is in charge of his or her personal information. An Indigo-Chapters loyalty program, for example, which requires customer disclosure of personal information for the company’s marketing department, goes almost overboard in terms of its transparency about consent, use and security. “Great care, though, has to be taken when manipulating sensitive data,” Horgan says. “The value of customer loyalty through privacy compliance is just too important.”

Oddly, few organizations have even considered that value. The first bank to employ an in-house privacy officer, RBC Financial Group, determined in 2000 that 7% of customer buying decisions with respect to personal banking was based on privacy. “You could take the market cap for that bank,” says Parker, “and you could figure out the value of the loss. It’s a lot.” As for online business, a Jupiter Communications Inc. study, Overview, Proactive Online Privacy, calculated that the Internet would lose some US$18 billion in 2002 due to privacy concerns.

It is no wonder that Chapters has expended extraordinary time and money updating and refining its online privacy statement to be something more than simply a protective legal disclaimer. Sievers plans to sample a number of online privacy statements and agrees that simple, clear and concise language is the key. “The point of the statement should be to reassure and draw the client in,” he says.

Satisfying both consumer trust and complex commercial/legal compliance will remain a struggle for years to come, Parker predicts. And CAs, once up to speed, will be in the centre of the fray. And he expects the privacy business to pick up dramatically with PIPEDA’s full implementation in 2004.

Australia’s Privacy Act, for example, has been in force since December 2001, covering both government and the private sector. Perhaps because the act there was not phased-in slowly like PIPEDA, its privacy commissioner has been inundated with more than 30,000 inquiries a year and about 1,000 formal written complaints. “We only had a couple of hundred complaints last year,” says Parker, “but when people become aware of their rights, it’ll happen.”

McKendry is ready for the onslaught and confident the accounting profession will have a pivotal role to play as businesses struggle to comply. “People will take comfort that there has been an independent verification by credible professionals about their compliance with good privacy practices,” he assures. As for Sievers, January 1, 2004 can’t come soon enough. “I take no comfort in this business of waiting to see if we’re deluged with client questions about the act and our ability to comply,” he says dryly. “It’s like an axe waving over your head. Let’s do it and get it right.”

How to achieve compliance

by Erin R. Kuzz

In practical terms the first step toward compliance is to designate one or more individuals responsible for privacy compliance. This privacy officer must have the training, resources, authority and budget to develop and implement compliant policies and procedures. Organizations must then determine precisely what personal information they collect, use and disclose. This will involve an internal audit the breadth and extent of which will depend upon the complexity of the organization and the work it undertakes. Larger organizations might consider establishing a working group representing input from various areas of the organization. A basic audit should identify the following:

1. Personal information about customers and employees collected and retained. Points where personal information may be routinely collected include: point-of-purchase, contests, e-mail, surveys, video cameras, audio tapes, marketing lists, loyalty programs, delivery services, warranties, returns, application forms, websites, call centres, technology enablers, employment applications and benefits applications.
2. What personal information is used in carrying out business, for example, in sales, marketing, fundraising and customer relations.
3. What personal information the organization obtains from, or disclose to, affiliates or third parties, for example in payroll outsourcing or benefits provider.
4. That appropriate protocols are in place to ensure continued protection where personal information is disclosed to a third party.
5. For what purpose personal information is collected.
6. To whom personal information is disclosed.
7. What forms of consent are employed.
8. The impact of PIPEDA, and/or provincial privacy requirements, on the organization (a legal interpretation may be required).
9. How the business plan addresses the privacy of personal information.
10. Adequate resources are allocated for developing, implementing and maintaining a privacy program.
11. What privacy policies the organization has established with respect to the collection, use, disclosure, retention and destruction of personal information.
12. How policies and procedures for managing personal information are communicated to employees.
13. How management and employees with access to personal information are trained in privacy protection.
14. How personal health information is collected, used, disclosed, stored and destroyed.
15. That appropriate forms and documents are fully developed.
16. Mechanisms are in place to ensure affected individuals are aware of the organization's privacy policies, including the rights to access personal information and if necessary to correct it.
17. The organization efficiently and effectively identifies and locates personal information about an individual.
18. To comply with established privacy policies, what specific objectives have been set for the organization.
19. To what extent have appropriate privacy control measures been identified and implemented.
20. How the effectiveness of the privacy control measures is monitored and reported.
21. What mechanisms are in place to deal effectively with failures to properly apply the established privacy policies and procedures.
22. How the organization will benefit from a comprehensive assessment of the risks, controls and business disclosures associated with personal information privacy.

Erin R. Kuzz is a partner with the law firm Sherrard Kuzz LLP in Toronto, specializing in advising and representing management on labour, employment and privacy law. She can be reached at www.sherrardkuzz.com. Rob Colapinto is a freelance writer based in Toronto.