SHERRARD KUZZ LLP
Barristers & Solicitors

Management Counsel

Employment and Labour Law Update
August 2003 Vol. II No. 4

PRIVACY COMPLIANCE HAS BUSINESS ADVANTAGES

In our November 2002 edition of Management Counsel we discussed the Personal Information Protection and Electronic Documents Act ("PIPEDA"), its purpose, effect and potential effect on federally and provincially regulated organizations. We also discussed the status of legislation or proposed legislation in the provinces and suggested that an Ontario act would be forthcoming shortly. We promised to keep you apprised.

It is now nine months later and while some things have remained unchanged others have not. PIPEDA continues to apply to the collection, use and disclosure of personal information in the course of federally regulated commercial activity. As well, on January 1, 2004 PIPEDA will apply across Canada to all personal information collected, used or disclosed in the course of commercial activity by any "organization" unless a "substantially similar" provincial privacy law is in force.

What then is the status of the respective provincial privacy legislation, or proposed legislation?

THE PROVINCES

As of January 1, 2004, in a province where privacy legislation "substantially similar" to PIPEDA is not enacted, PIPEDA will govern every organization engaged in commercial activity.

As of the Privacy Commissioner's first report to Parliament in May 2002, only Quebec had enacted "substantially similar" legislation.

Since then, each of the Maritime Provinces has indicated that it does not intend to introduce provincial privacy legislation, and will apply PIPEDA come January 1, 2004.

In 2002 the Government of Ontario circulated draft privacy legislation and reportedly received some 600 submissions from the public. It had been the Government's intention to enact privacy legislation by the end of 2002. However, to date, the Government has not tabled an amended bill and has indicated no timetable for introduction. With a provincial election looming on the horizon, time may be running out and it is very possible that Ontario will not pass its own substantially similar legislation prior to January 1, 2004. In that event, Ontario will become subject to PIPEDA.

> *"...protection of privacy only because the law requires it fails to recognize the benefits that privacy protection can bring to an organization."*

Two provinces have introduced privacy legislation - British Columbia (Bill 38, the Personal Information Protection Act) and Alberta (Bill 44, similar to British Columbia's Bill). Largely similar, both Bills were introduced in May, 2003. However, within days, then Federal Privacy Commissioner George Radwanski raised serious concerns about what he found to be inferior protections with regard to certain "consents" and the failure to provide adequate opportunity to access and correct personal information.

Among Mr. Radwanski's criticisms of the proposed British Columbia and Alberta legislation was that they offered (what he considered) inadequate protection for personal information of private sector, provincially regulated employees in the context of employment-related activities. This is a curious finding given that absent provincial privacy legislation, PIPEDA does not protect this type of personal information (non-federally regulated, private sector employee personal information used in the context of employment-related activities). Neither province has indicated whether or to what extent it intends to table amended legislation.

THE COST OF NON-COMPLIANCE

While legal compliance is the first and most obvious reason for implementing policies and practices in accordance with legislated privacy principles, protection of privacy only because the law requires it fails to recognize the benefits privacy protection can bring to an organization.

Effective privacy compliance is now 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.

In that the Federal Privacy Commissioner is permitted to make public the names of offending organ-

continued inside

Management Counsel

PRIVACY...

Continued from p.1

izations (where he deems it to be in the public interest to do so), the result may be devastating to an organization's reputation vis-à-vis its brand, customers, business partners and employees. For example, some organizations seeking to be privacy compliant have already 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 otherwise necessary for efficient business practices and product development.

The benefits of protecting privacy are therefore more obvious when organizations understand how customers (and 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.

An example is the case of Air Canada's Aeroplan™ program. In March, 2002 the Federal Privacy Commissioner publicly released his findings that the program violated the privacy rights of individuals in a number of ways, including the failure to provide what he considered to be clear and appropriate consent provisions. The Aeroplan program allowed patrons to "opt-out" of information sharing among Aeroplan affiliates and other organizations by checking a box and returning a form to Aeroplan. In his press release, which was also posted on his website, the Commissioner stridently accused the opt-out format of being a "weak form of consent reflecting at best a mere token observance of what is perhaps the most fundamental principle of privacy protection."

WHERE TO FROM HERE?

Whether under PIPEDA or "substantially similar" provincial legislation, compliance with privacy legislation is a reality. For federally-regulated organizations this has been the case for years. For others, January 1, 2004 is fast approaching.

An effective privacy program needs to be integrated into the corporate culture. Its implementation will take time, effort and money. In order to succeed it is essential that privacy protection become a corporate priority for all levels of every organization. Top level commitment is critical.

The first step toward compliance is to learn about PIPEDA and the patchwork of privacy legislation across North America and, in some cases, the world. This is a complex task that will require ongoing partnership with individuals having expertise in the area. It is absolutely necessary that organizations educate themselves. Any organization that does not take this issue seriously does so at its peril.

The second step toward compliance is to designate one or more individuals responsible for privacy compliance. The "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. What personal information about customers and employees does the organization collect and retain? For example, points where personal information may be routinely collected include:

Point-of-purchase, Contests, Email, Surveys, Video cameras, Audio tapes, Marketing lists, Loyalty programs, Delivery services, Warranties, Returns, Application forms, Web sites, Call centres, Technology enablers, Employment applications, Benefits applications

continued at right

Breakfast Seminar

Our employment and labour law update seminars will be resuming in the autumn. Please join us for:

TOPIC: "Open Microphone - Answers to All Your Labour & Employment Questions"
DATE: Wednesday, September 24, 2003, 7:30 a.m. – 9:00 a.m.
(program to start at 8:00 a.m.; breakfast provided)
VENUE: Wyndham Bristol Place Hotel, Toronto Airport
950 Dixon Road, Toronto

HRreview Seminar Series

Watch for your faxed invitation the week of August 4th, 2003 or call 416.603.0700 to request an invitation.

2. What personal information is used in carrying out business, for example in sales, marketing, fundraising and customer relations?

3. What personal information does the organization obtain from, or disclose to affiliates or third parties for example in payroll outsourcing or benefits provider?

4. Are appropriate protocols in place to ensure continued protection where personal information is disclosed to a third party?

5. For what purpose is the personal information collected?

6. To whom is personal information disclosed?

7. What forms of consent are employed, if any?

8. What is the impact of the PIPEDA, and/or provincial privacy requirements, on the organization (a legal interpretation may be required)?

9. How does the business plan address the privacy of personal information?

10. Are adequate resources allocated for developing, implementing and maintaining a privacy program?

11. What privacy policies has your organization already established with respect to the collection, use, disclosure, retention and destruction of personal information?

12. Where there are employees, how are the policies and procedures for managing personal information communicated to them?

13. How is management and employees with access to personal information trained in privacy protection?

14. How is personal health information collected, used, disclosed, stored and destroyed?

15. Are the appropriate forms and documents fully developed?

16. What mechanisms are in place to ensure that affected individuals are aware of the organization's "privacy policies", including the rights to access personal information and if necessary to correct it?

17. How is the organization able to efficiently and effectively identify and locate personal information about an individual?

18. To comply with established privacy policies, what specific objective have been set for the organization?

19. To what extent have appropriate privacy control measures been identified and implemented?

20. How is the effectiveness of the privacy control measures 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 would your organization benefit from a comprehensive assessment of the risks, controls and business disclosures associated with personal information privacy?

For some organizations becoming privacy-compliant will be daunting and costly. For others it will be undertaking a relatively straightforward audit and compliance program. Either way, the potential cost of non-compliance is simply too high.

Sherrard Kuzz will continue to monitor these developments and will keep you informed. We also encourage employers to take steps now to prepare for the application to their workplaces of the obligations of privacy legislation.

Our lawyers have expertise assisting our clients in this regard. If you would like to discuss these issues with us, please contact any member of our legal team.

DID YOU KNOW...?

That the Federal Government has expressed an intention to create criminal liability for health and safety violations? Read more about it in the next edition of *Management Counsel* or contact any member of the *Sherrard Kuzz LLP* team for more details.

ANTI-SPAM LEGISLATION GAINING GROUND WORLDWIDE

SPAM!

Two years ago "spam", unsolicited electronic mail attempting to sell a product or service, accounted for approximately 10% of internet traffic. Today that number is more than 30% and growing. A study by the European Commission estimates the cost of abusive e-mailing to exceed 10 billion Euros ($14 billion Cdn.) a year.

A number of jurisdictions have passed legislation to address the problem of spam. Japan's legislation requires anyone sending an e-mail for commercial purposes to clearly identify this in the subject line of the e-mail. It also requires the sender to provide its contact information in the e-mail, and prohibits the sender from sending further e-mails to anyone who chooses to opt out of receiving them. Violators may be fined or jailed. The law also prohibits businesses from sending large numbers of advertising e-mails to addresses randomly chosen by computers.

More than half of American states have some sort of "anti-spam" law. Nevada led the way, introducing legislation in 1997. Since then, state laws provide varying levels of protection. In Utah, anyone sending unsolicited commercial e-mail through an internet service provider in Utah, or to any resident of Utah, must include the sender's name and physical address in the e-mail. Most states require some type of identification in the subject line that the e-mail is of a commercial or advertising nature, and require an opt-out process for recipients.

In Canada, there are no laws expressly prohibiting "spamming". Distribution of unsolicited promotional and product information, in print form or over electronic networks is not illegal nor is it directly regulated.

However, for organizations to which it applies, the Personal Information Protection and Electronic Documents Act ("PIPEDA") regulates the collection, use or disclosure of personal e-mail addresses without consent. It is therefore a violation of PIPEDA to send "spam" to a personal e-mail address, or to sell a personal e-mail account without the individual's consent. Unfortunately, there is no similar protection for a work-related e-mail address.

The Government of Canada has issued a Discussion Paper on e-mail marketing (www.e-com.ic.gc.ca) and has invited comments.

One final caution: some spammers who provide an "opt-out" opportunity (i.e. "type 'unsubscribe' in the subject line to remove your name from our database") use your response to ensure they are sending spam to a live e-mail account, not for the stated purpose. In those circumstances, you may be setting yourself up for even more spam in the future.

SHERRARD KUZZ LLP
Barristers & Solicitors

155 University Ave., Suite 1500
Toronto, ON Canada M5H 3B7
Phone: 416.603.0700
Fax: 416.603.6035
www.sherrardkuzz.com
info@sherrardkuzz.com

Michael G. Sherrard
Direct: 416.603.6240
msherrard@sherrardkuzz.com

Erin R. Kuzz
Direct: 416.603.6242
erkuzz@sherrardkuzz.com

Thomas W. Teahen
Direct: 416.603.6241
tteahen@sherrardkuzz.com

Madeleine L. S. Loewenberg
Direct: 416.603.6244
mloewenberg@sherrardkuzz.com

Shelly M. Patel
Direct: 416.603.6256
spatel@sherrardkuzz.com

Ronald J. Ouellette
Direct: 416.603.6254
rouellette@sherrardkuzz.com

Providing management with practical strategies that address workplace issues in proactive and innovative ways.

Management Counsel is published six times per year by Sherrard Kuzz LLP. It is produced to keep readers informed of issues which may affect their workplaces. *Management Counsel* is not intended to provide specific legal advice. If readers wish to discuss issues raised in this publication or any other labour or employment-related issue, they are encouraged to contact legal counsel.