by John Wunderlich

THE COST OF PRIVACY

Whether you are directly mandated with protecting employee privacy or you are responsible for payroll and must therefore ensure payroll privacy requirements are met, you will find yourself in discussions from time to time with other departments that wish to have access to sensitive information.

The reasons for requesting access vary. It may be to mitigate risk, especially if your organization has a coherent risk management policy, or it may be compliance related, particularly where your organization operates in a regulated environment. Both of these reasons—and they are not mutually exclusive—centre around avoiding negative impacts on the organization. This approach means that the minimum resource investment required to avoid potential harm is the investment that will be made. This is the cost of privacy for risk management or compliance purposes.

When an organization evaluates its privacy risk to determine the cost of compliance, it must consider the potential cost in both human and financial resources of failing to meet its privacy objectives. As a matter of rational business practice, the cost associated with ensuring that privacy is protected will not exceed the eventual cost of failing to do so. A number of decisions made by privacy commissioners and federal and provincial courts in 2010 have helped to qualify this potential human and financial cost.

If an employee whose privacy complaint to the federal Privacy Commissioner is determined to be well-founded wants monetary damages, he or she must seek redress in the Federal Court. Decisions in two such cases were made last year.

In the first case (*Randall v. Nubodys Fitness Centres*), the employer paid half of the employee's monthly fee at a fitness club. The employee complained that his privacy had been breached with the fitness club because attendance records were shared with the employer, and the employer talked about this information in a meeting. The Privacy Commissioner and the Federal Court agreed that this was a privacy violation, as no consent had been obtained to share the information.

In the second case (*Stevens v. SNF Maritime Metal Inc.*), the employee was terminated from a scrap metal operation when his employer learned from a customer that he had opened an account with that customer to sell scrap metal as well. The employee complained that by divulging his account information to his employer, that customer had violated his privacy rights. Again, the Privacy Commissioner and the Federal Court agreed there was a breach.

In both of these cases, no monetary award was given to the former employees. In the first case, the Court determined that the violation of privacy was not serious enough to warrant damages. The judge stated, "Pursuant to section 16 of the PIPEDA [*Personal Information Protection and Electronics Document Act*], an award of damages is not be made lightly. Such an award should only be made in the most egregious situations. I do not find the instant case to be an egregious situation." In the second case, the Court argued that the source of the complaint was the loss of employment after being terminated for cause. Here, the judge stated, "The PIPEDA right of action is not an end run on existing rights to damages." The net affect of these decisions, in the words of Michael Geist, a law professor and blogger on these kinds of issues, is to set a high bar for the awarding of damages for privacy.

However, the lack of monetary damages awarded in these cases does not diminish the importance of privacy protection. Two Alberta Privacy Commissioner decisions last year—one directly related to payroll information—emphasize the risks of real and significant harm and the employer's responsibility. In these cases, the issue was whether the organizations were required to notify individuals when their privacy had been breached. In 2010, breach-reporting and notification requirements were added to the Alberta privacy law, which force organizations to notify Alberta's Privacy Commissioner when individuals' personal information be lost or improperly accessed, and a reasonable person would view the inci-

dent as presenting "a real risk of significant harm" to an individual. These decisions illustrate how these requirements would be applied in practice.

In the first case (OIPC P2010-ND-001), an employer in the U.S. found a small number of underwriting files and other documents containing personal information outdoors near its headquarters. Since some of the files concerned individuals were Albertans, the Alberta Privacy Commissioner had jurisdiction. In the second case (OIPC P2010-ND-002), unbeknownst to the employer, its storage facility in Alberta was disposed of and payroll records were found in a dumpster. In both cases, the Commissioner found that the information "could be used to cause significant harm to individuals" and "provides comprehensive individual profiles that could be used for identity theft and/or fraud." As a result, both organizations were required to notify the affected individuals of the breach.

What do these decisions mean for the cost of privacy in payroll? They confirm that payroll information constitutes a high privacy concern and that as a best practice individuals should be notified when their payroll privacy is breached, particularly where the breach is an unauthorized disclosure. Left to be determined is whether the breaches in Alberta, which were considered quite serious because of the real risk of significant harm, would rise to the Federal Court's level of "egregious" and qualify for monetary damages. To hedge this risk (and reduce the potential cost to the organization), payroll professionals must ensure that they have mature security practices and a robust privacy program in place. ■

John Wunderlich is an information privacy and security consultant, based in Toronto. For more information, check out his intermittently updated website at http://compliance.wunderlich.ca.

Notice: This column reflects solely the opinions of the author. Individuals are encouraged to seek qualified legal advice on points of law or matters of interpretation.