TECHNOLOGY

By Al Doran, CHRP

PRIVACY: THE NEXT GREAT CHALLENGE FOR HR

There has been a great amount of interest in this topic of late. So when an opportunity came up recently to sit in on a full morning seminar with two experts in the field, I jumped at the chance. The problem is, after listening to the two speakers for several hours, I am convinced that this is a work in progress and possibly one of the biggest challenges that human resources will face over the next few years.

I am starting to get the same worried feeling I got in the early 1990s when we were faced with pay equity in Ontario. Legislation based on a good cause, but ill thought out as to how one would ever implement it. Well, it appears that privacy legislation may provide us with similar challenges and at least as much ambiguity going into it.

Let's face it, if you have been a human resources professional in Canada for more than five minutes, you already have learned to take great care in how you treat personal information. From the job applications you handle to the T4 slips you produce each February, you manage the information with caution and do not give it to anyone who does not have a legitimate need to see it. But is that enough these days? Not nearly.

First off, let me state that anything I say in this article is not to be construed as legal advice. (See, a morning of listening to two lawyers does strange things to you).

A lot is changing, thanks in large measure to two levels of privacy legislation, one federal, one provincial.

The Personal Information Protection and Electronic Documents Act received Royal Assent on April 13, 2000. The purpose of the act is to protect the privacy of personal information that is collected, used or disclosed in the private sector, to permit business to be conducted with the federal government by electronic means, and to clarify how electronic records may be used as evidence. Part 1 of the act, entitled "Protection of Personal Information in the Private Sector," came into effect Jan. 1, 2001, 2001. Its application to specific organizations and to types of personal information will occur in several stages. Stage three comes into effect on Jan. 1, 2004, when the act will apply to all organizations in Canada. Keep in mind there will be similar provincial legislation, but more on that later.

There are many "principles" in the federal act that are termed "voluntary," yet they include the word "should" in many cases and the word "recommendation" is overworked as well. Case in point: "Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information."

The basic right of the act is pretty simple: "Provide individuals with a right to privacy concerning their 'personal information.'" The basic principal is that personal information should not be collected, used or disclosed, without the prior knowledge and consent of the individual concerned, subject to limited exceptions.

"Personal information" is very broadly defined and will ultimately lead to some arguments and confusion, but keep in mind this is a work in progress. The full weight of the act is not expected to be felt until many issues are tested in the courts. As an example of the confusion, an exemption for the "personal information" includes name, title, business address or telephone number of an employee. And it may even include an employee's name, home address and phone number if it's in a public phone book.

What are some of the immediate concerns?

One major concern is the potential sale of your company's employee database to third parties without the consent of each and every employee. Before you say, "We do not do that," think about it for a moment. Do you ever provide your insurance carrier with a copy of that database so it can mail a special offer to your employees? This may now be a problem, especially if that mailing is from a province other than the home province of the employee.

And what about company documents, whether corporate or personal? One would think that the memos, e-mails and reports written by an employee would be the property of the company who paid the employee, right? Maybe not, if the employee did not give his/her direct permission to use them, they may not be corporate material after all.

The role of the word "consent" in the act. There are so many different applications and interpretations of the word "consent" in the act that you truly need a lawyer to sort it out. There is "meaningful consent," where the purposes must be stated such that the individual can "reasonably understand" how his/her information will be used. There is "ongoing consent," where the employee may withdraw consent. Then there is "consent to transfer information," and the question of whether this gives the company permission to pass along a copy to a third

party. And we have "express vs. implied forms of consent," where express consent is recommended for very sensitive personal information such as health information, but implied consent may be adequate for less sensitive information.

Many companies are going to find that they will have to implement very sophisticated and time-consuming consent tracking systems to determine who consented when and for what purposes.

The act states that each organization is responsible for personal information under its possession or custody, including information transferred to a third party for processing (payroll, benefits, etc.). An organization is therefore (i) required to designate an individual to oversee the organization's compliance privacy principles and (ii) to adopt policies, practices and procedures to give effect to the principles, including developing information and training staff about the organization's policies, practices and procedures.

Every company strives to have up-to-date and accurate human resource information. Now, under the act, companies are required to do this. It must be so (i) for the "identified purposes," and (ii) to minimize the possibility that inappropriate information is used to make a decision about the individual. This has pretty deep meaning beyond what is obvious off the top. It means that if you collect information on employees related to a life insurance project, you cannot use that information in assessing their "creditworthiness." The information must also be held long enough for the employee to have access to that information after a decision is made. The act does not state how long that should be. A very important note: an organization is prohibited from "routinely updating" personal information, unless that is necessary for the "identified purposes." All of a sudden, I can see where a well thought-out HRMS with employee self-service, linked to sign-off forms is going to play a major role in your future.

Again, we as HR professionals always take pride in what we do to protect the privacy of information related to our employees – but this may no longer be enough. We must protect the information physically and electronically and we must inform the employees of the steps taken. Each organization must make sure that every employee has access to his or her own information and employers must have procedures in place to deal with inquiries and complaints.

The act and compliance will be monitored by the federal government where a privacy commissioner, who has reasonable grounds, may audit any company thought to be in non-compliance. Organizations being audited should absolutely be represented by qualified counsel. The commissioner has broad powers to summon and compel witnesses, enter premises, examine records, and disclose information regarding an offense.

What are some of the key things a company should be doing to stay in compliance?

1. Understand your current practices regarding the collection, use and disclosure of personal information.
2. Codes of practice: develop and comply with a privacy code.
3. Appoint a privacy officer for your company.

For more information on the federal legislation, visit www.privcom.gc.ca.

Ontario's consultation on privacy protection

Ontario is implementing its own legislation. The Ministry of Consumer and Business Services recently released a draft of the Protection of Privacy Act, 2002, in which the Ontario government attempts to address some of the ambiguities of the federal legislation. The province has already identified a lot of gray areas for further discussion, such as home e-mail address of an employee: personal or organizational? A consultation period on the draft legislation had been scheduled over the early spring.

Visit www.cbs.gov.on.ca/mcbs/english/56HK6V.htm for more information.

Clearly, there is a lot to come in this area and we should be getting ready for it now. □

Al Doran, CHRP, is president of Phenix Management Int'l, a Toronto management consulting firm specializing in HRMS issues. He is co-author of Human Resource Management Systems: A Practical Approach*, published by Carswell. www.hrmsbook.com. He is a member of the board of directors of both IHRIM and CCHRA. He may be reached at aldoran@pmiHRM.com and his home page is www.pmihrm.com.*