# Private act

**Over the past few years, there has been a lot of confusion about privacy legislation. Who does it apply to? When is it really coming? How much impact will it have? Busy engineers need to know what privacy legislation means for them. For example, one sleeper issue for many engineers is that there will be restrictions on their ability to search for personal information on public databases about prospective individual clients without their consent. Here's what's in store.**

by Richard Steinecke, LLB

For almost all engineers, the federal *Personal Information Protection and Electronic Documents Act* takes effect this coming January. Ontario has circulated a draft *Privacy of Personal Information Act*, but it is highly unlikely that it will be enacted before this January. Engineers covered by the federal privacy act need to have their policies and procedures in place by then.

The act is intended to cover the entire private sector. With very few exceptions, the privacy act applies to anyone who carries on "commercial activities." That will include most engineers. Even if the government pays for the goods or services, the privacy act will likely apply. Only engineers employed by a government body or a non-profit agency that does not sell goods or services may be exempt.

The privacy act applies to any collection, use or disclosure of personal information. "Personal information" means any information about an identifiable individual that relates to their personal characteristics (e.g. gender, age, income, property, home address or phone number, social insurance number, ethnic background, education, family status), their health (e.g. health history, health conditions, health services received by them) or their activities and views (e.g. dealings with the engineer, opinions expressed by an individual, religion, political involvement, an engineer's view or evaluation of an individual or their property). Personal information is to be contrasted with business information (e.g. an individual's business address and telephone number) which is not protected by the act.

## What has to be done?

Each organization must appoint an information officer and develop and publish its privacy policy. The information officer should be a senior person in the organization. The information officer can be an outsider hired by an organization to perform this role, but that may make it more difficult for the organization to develop a privacy policy that fits its office or practice.

The information officer is responsible for overseeing an organization's compliance with its privacy obligations. An organization's privacy policy should cover the following issues:

- reviewing the organization's policies and practices for collecting, using and disclosing personal information (including conducting an audit of the current personal information practices of the organization);
- implementing procedures to safeguard personal information;
- ensuring individuals have the right to access and correct any personal information about themselves held by the organization;
- implementing a retention and destruction of information policy;
- training the organization's staff;
- acting as a contact person for inquiries from the public or clients; and
- ensuring there is a process for handling complaints made about the organization's information practices.

Engineers must also make sure that their organization has privacy policies dealing with all of these issues. These policies must be made available to the public. This public access obligation might be met by posting the policy on the organization's website or in its reception area. Alternatively, a copy can be provided to new clients on their first visit and to anyone else upon request. The policies have to be understandable as well.

Privacy policies apply on an "organizational" level. Often, the identity of the organization is obvious because the sole practice, partnership or corporation is well defined. But where a group of people or entities work together in a loose affiliation, there may be more than one way to define the organization. Engineers and their business associates can then decide who their organization will be. For example, every engineer can have his or her own privacy policy. Or, engineers working with others can join together to form a broader organization with one privacy policy covering them all. It just depends on what is most convenient for everyone. Everyone within an organization has to agree to be monitored by the information officer. Also, organizations will need special consent to disclose personal information outside of the organization.

## What are the restrictions?

As a general rule, engineers need to obtain informed consent for the collection, use and disclosure of personal information.

This consent is distinct from the consent for providing services. Like any consent, it can be obtained in writing, orally or by implied consent. In the traditional circumstance of an engineer collecting information directly from the client solely for the purpose of providing services to the client, consent may be implied. But any departure from this simple approach creates some new obligations for obtaining informed consent. In real life, the simple approach is not usually enough.

Areas in which some change may be required include the following:

- where the engineer collects information about other individuals (e.g. about the client's family members or the client's own clients);
- where the engineer collects information about the client from other persons (e.g. from previous engineers for the client, almost any public database, from family members of the client, from the client's business contacts);
- where the engineer collects information to be shared with others who are also advising or providing services to the client (i.e. a team approach);
- where there is the likelihood of an ongoing relationship and the information will be used for ongoing services, especially if this is not obvious to the client (e.g. collecting a broad background of a client's financial situation to ensure that one can provide broader services later on);
- where third parties will have access to the information (e.g. for legal, billing or financing purposes);
- where the engineer will use the information for related purposes (e.g., for billing the client or a third party later);
- where the engineer will use or disclose the information for secondary purposes (quality control by the organization, regulatory accountability); and
- where the engineer might sell the practice or business later on and will need to provide prospective purchasers with access to client information to help the purchaser conduct a due diligence review.

In any of these circumstances, the engineer should at a minimum explain the purposes for which the information is being collected and obtain some form of consent. Often, the consent process can be a brief oral discussion with the client. Giving the client a handout setting out the engineer's usual information practices and checking with the client that he or she understands the handout would often be sufficient. Alternatively, obtaining a written consent at a client's first visit may work in many circumstances. While the Information and Privacy Commissioner is leery of obtaining blanket consents, it may be that, for the usual private practice, this may be appropriate and sufficient.

There are some exceptions that permit engineers to collect information without consent. The most common example is where the purpose is to investigate a breach of law or contract and obtaining consent would compromise the investigation (e.g. a fraud by a client; helping a client deal with a contractual dispute with a third party). Certain emergency situations (e.g. medical crisis) may permit the collection, use or disclosure of information without consent as well, but that would be rare for an engineer.

Engineers are also obliged to collect the least amount of personal information that is consistent with the purposes for which it was collected. For example, collecting an individual's Social Insurance Number is usually not necessary. One should not routinely collect a client's home address (unless the client wants something to be

## WHAT THE ACTS SAY

The *Professional Engineers Act* is a provincial statute. Under the Canadian constitution, provinces have jurisdiction over property and civil rights; the federal government has jurisdiction over matters that involve inter-provincial and national affairs. The federal privacy act is federal legislation, which at first glance would not be of much concern to a practitioner in Ontario.

But there are certain aspects of an engineer's practice that may involve transactions that cross provincial jurisdictional boundaries. Examples include international marketing on the Internet and collecting personal information, working as an employee collecting personal data for a federal undertaking located in this province, such as airlines and airports, railways, banks, or managing information submitted from prospective employees located outside Ontario. The federal privacy act includes three crimimal offences punishable by fines of up to $100,000 on indictment. The offences are:

1. knowingly failing to maintain personal information that is subject to an access request;
2. knowingly disciplining, dismissing or harassing a whistle blower or an employee who refuses to contravene the privacy act; or
3. obstructing the commissioner in the course of an investigation or an audit.

If the federal privacy act is applicable to your practice, failure to comply may also result in a disciplinary complaint being filed by a member of the public being affected by a breach of information privacy.

Practitioners are reminded that under section 72(2)(d) of Regulation 941 under the *Professional Engineers Act*, a failure to make responsible provision for complying with applicable statutes, regulations, standards, codes, by-laws and rules in connection with work being undertaken by or under the responsibility of the practitioner may be considered professional misconduct.

In addition, the Code of Ethics at section 77(3) states that a practitioner shall act in professional engineering matters for each employer as a faithful agent or trustee and shall regard as confidential, information obtained by the practitioner as to the business affairs, technical methods or processes of an employer.

The above violations can result in a licence suspension or revocation, or fines up to $5,000.

In response to the federal privacy legislation, and in order to boost consumer and business confidence since the advent of the World Wide Web, broad new provincial privacy legislation is expected in Ontario soon. It will largely mirror the federal act but will go further in that it would apply to non-commercial organizations (such as PEO) and to employee information held by provincially regulated employers.

*— Dwight Hamilton*

sent there, or that is the project site). Engineers should not collect financial information about a client who pays the full account in advance.

## What safeguards are needed?

Most engineers are already careful to preserve their client's confidentiality. When setting out the safeguard policies in writing, engineers may wish to review some of their practices, however. For example, can people see confidential files or computer screens when walking through the office or business? Is all personal information shredded before being put in the recycling box? The Information and Privacy Commissioner strongly disapproves of sending personal information through regular email over the Internet.

A fundamental principle of the act is that any individual has the right to request and see any personal information engineers hold about them. In fact, engineers are required to help individuals make such a request (e.g. explain the filing system so the person knows what to ask for) and to assist them in understanding the information (e.g. explain abbreviations and technical terms). There are a few exceptions where access can be restricted (e.g. where the disclosure will reveal personal information about another individual or will reveal trade secrets), but these are narrow. Engineers will also have to tell individuals to whom the organization has disclosed the personal information about them.

If the individual believes any of the personal information is wrong, he or she can ask that it be corrected. The organization must correct any information it agrees is wrong. The organization must also notify any third parties who received the wrong information of the correction. Where the client and the organization cannot agree that an error has been made, the organization must record the disagreement and notify any third parties who received the contested information. Disagreements about corrections can be taken to the Information and Privacy Commissioner, who may review the situation.

Organizations must also have an internal complaints system to handle concerns about their privacy practices. The internal complaints system should have the following features:

- a designated individual in the organization (perhaps the information officer) to receive and ensure the prompt investigation and response to all complaints;
- an easily accessible and simple to use complaints procedure that at a minimum includes acknowledging receipt of the complaint, investigating it, and providing a decision with reasons;
- a process for the organization to respond appropriately to complaints that are justified including making changes to its privacy policies; and

- notifying the public of external recourses, including the engineer's regulatory body and the federal Information and Privacy Commissioner.

Engineers will be held accountable by both the federal Information and Privacy Commissioner and, to a lesser extent, by PEO, in respect of their compliance with the act.

The federal Information and Privacy Commissioner has oversight of the privacy act and functions as an ombudsman. The commissioner has the following responsibilities:

- investigating complaints about an organization's personal information handling practices, including entering the organization's premises and summonsing documents and witnesses;
- mediating and conciliating such complaints;
- auditing the personal information handling practices of an organization;
- making a public report of poor personal information practices by an organization;
- seeking remedies for a breach of the privacy act in the Federal Court of Canada.

Once the commissioner has issued a report, either the complainant or the commissioner can then apply to the Federal Court of Canada for one or more of the following remedies:

- an order for the organization to correct its personal information handling practices;
- an order for the organization to publish a notice of corrective action; or
- an award of damages for any humiliation of the complainant.

All indications are that the current Information and Privacy Commissioner tends to be educational rather than punitive in his enforcement style, particularly where it appears an honest mistake has been made. It is still better to avoid a complaint than having to deal with one, however.

PEO may also hold the engineer accountable for his or her privacy practices. Where the conduct involves a breach of core professional values, regulators will have an additional reason to take action. Even where core professional values are not breached, every engineer is generally obliged to comply with the law, especially those designed to protect the public or that reflect on the engineer's suitability to be a member of the profession. Many breaches of the privacy act by an engineer may warrant some regulatory action.

Richard Steinecke, LLB, will be a presenter at a seminar on getting ready for the new privacy legislation on November 7, 2003. The seminar will be held in Toronto and will include a step-by-step workbook that will assist engineers in developing and implementing privacy policies. See www.sml-law.com/privacy-seminar for registration details.