Privacy protection is good business

The development of a comprehensive policy on the treatment and use of personal information has involved all of PEO. The engineering regulator is acting voluntarily to show its commitment not only to new government expectations, but also to better protect an easily overlooked but increasingly important commodity.

PEO is proceeding apace with its internal privacy policy to bring the regulator in line with government and public expectations for the collection, use and treatment of personal information.

Driving the issue is the federal government's *Personal Information Protection and Electronic Documents Act* (PIPEDA), which came into force for all commercial organizations in January 2004. The legislation was drafted primarily in response to incidents of careless institutional use of personal information, particularly in the health and financial services sectors. The widespread use of Internet-based data collection and information exchange has also led to increased concern about the safeguarding of personal information.

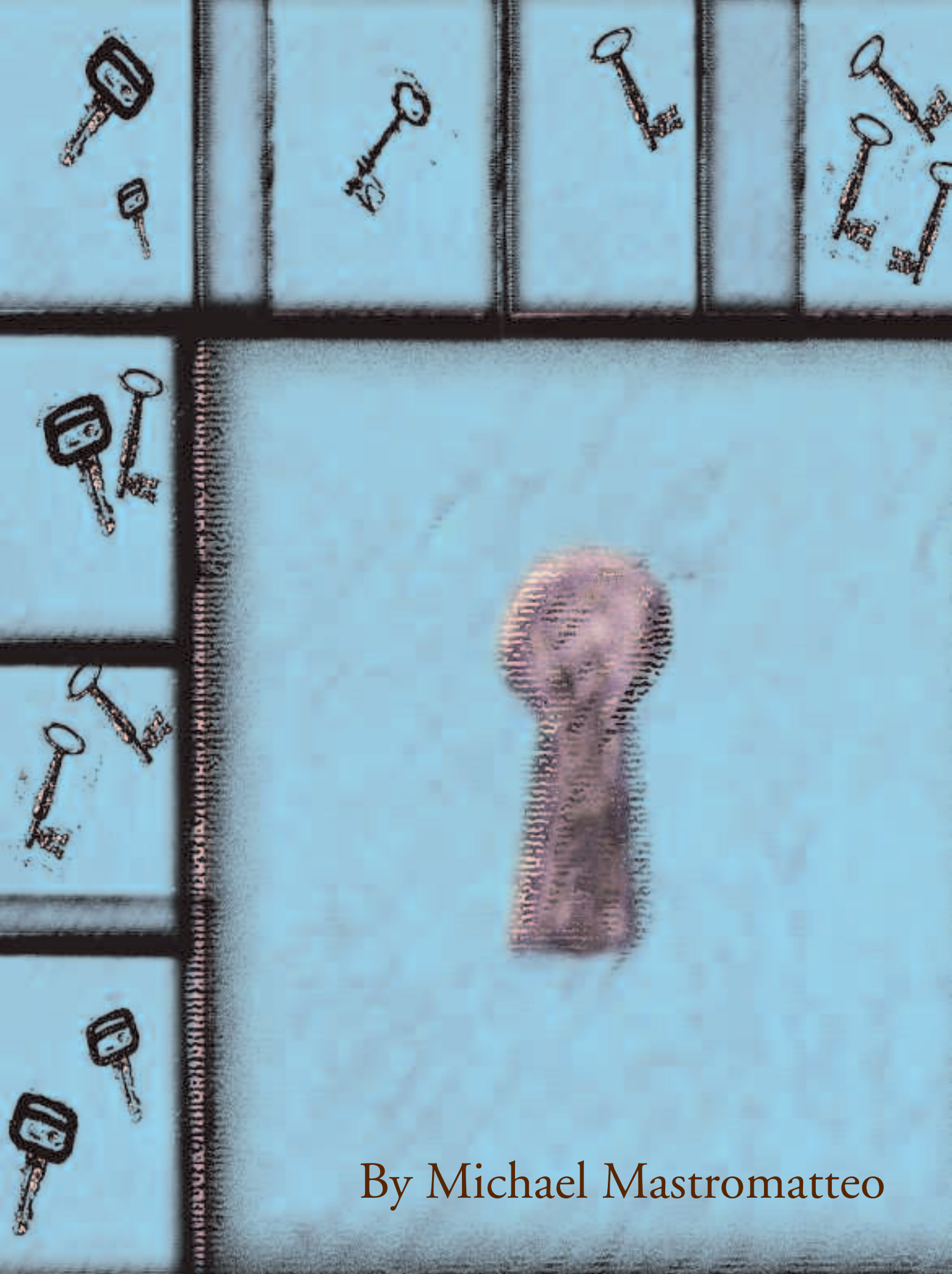
The legislation spells out how commercial organizations in the private sector are to treat personal information used in day-to-day business operations. PIPEDA does not apply to commercial activities in provinces that have enacted their own legislation covering personal information. It does hold sway, however, for interprovincial activities, or where no equally rigorous provincial legislation is in force.

Personal information is said to be anything that reveals characteristics about an individual, including gender, age, home address, telephone number, health history, social insurance number, religion or ethnicity. In some respects, the only information that might not be considered "personal" is what would appear on a typical business card.

The Ontario government is considering legislation similar to PIPEDA. In fact, PEO participated in a 2002-2003 consultation on a draft bill that did not go forward. Although provincial legislation covering personal information in the private sector is yet to be enacted, many organizations not covered by PIPEDA but that would likely be covered by a provincial law are in the process of voluntarily developing privacy policies and informing clients and the public that these policies are available.

Underlying principles

Because PEO is not strictly a "commercial organization," it is not covered by PIPEDA. Nonetheless, PEO privacy policy is founded on PIPEDA's 10 underlying principles (accountability; identifying purposes for collecting personal information; obtaining consent for collection, use and disclosure of personal information; limiting collection of personal information; limiting use, disclosure and retention of personal information; ensuring accuracy of personal information; safeguarding personal information; being open about policies and practices for dealing with personal information; providing access to information held about an individual; and establishing a mechanism for



By Michael Mastromatteo

PEO has always treated personal information

individuals to challenge an organization's handling of their personal information (see *Engineering Dimensions*, January/February 2004, p. 14 and November/December 2004, p. 22).

PEO has also developed protocols for sharing information about members internally. The ultimate test for internal sharing of information is the "need-to-know" principle. If there is a clear need for a staff member to know information that will assist PEO in its regulatory function, that information will be shared. Personal information that is unconnected to PEO's regulatory function will not be shared.

Kim Allen, P.Eng., registrar and chief executive officer, said PIPEDA has provided more incentive for PEO to build additional safeguards into its treatment of personal information. It has always followed a cautious approach to collecting and using personal information, but the development of a comprehensive privacy policy has resulted in a systematic review of the process.

Allen has been appointed PEO's chief privacy officer. In that role, he will investigate complaints from individuals on any matters involving PEO's disclosure or use of personal information. PEO will address each privacy-related complaint and make any necessary changes to its internal privacy policy.

In an October letter to staff and volunteers, Allen described PIPEDA as an attempt to balance an individual's right to privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes. "Our privacy policy is a statement of the principles and guidelines for the minimum required protection of personal information collected, used or disclosed by PEO staff, committees or chapters," Allen said.

Some of the other provincial engineering regulators are ahead of PEO in this area, largely as a result of provincial legislation already being in force. For the most part, provincial privacy legislation is based on the same 10 principles as are contained in PIPEDA, which is, in turn, based on the Canadian Standards Association's *Model Code for the Protection of Personal Information*.

Professional engineers working with companies that fall within the "commercial organization" category will be required to operate under PIPEDA's new privacy expectations. An organization is defined as a single individual, a partnership, a corporation, or an association of individuals or partnerships.

To align its operations with the public's increased privacy expectations, PEO has devoted considerable resources to writing its privacy policy and educating staff about the appropriate handling of personal information. In addition, a PEO project management team has reviewed existing internal procedures for data collection, revised appropriate forms and documentation, and surveyed employees as to their general knowledge of privacy issues.

Irena Langenfelds, PEO's document management supervisor, is project manager for the privacy policy implementation. She says the association has established a six-month timeframe, from October 2004 to March 2005, to implement the project. In April 2004, PEO engaged the services of privacy policy consultants Richard Steineke and Lisa Braverman, of law firm Steineke, Maciura LeBlanc, to review its needs and help draft its privacy policy.

More awareness

"By the number of phone calls received, it appears that many PEO members and members of the public are becoming more aware of the privacy policy and privacy issues," Langenfelds said. "That certainly provides us with additional incentive to stay on schedule with each part of the implementation project. The bottom line for our policy, and for those of most organizations, is to be open about why information is being collected and, above all, not to release personal information."

For the most part, personal information is collected for such purposes as membership, licensing, and volunteer or chapter activity. Staff collecting personal information must explain why it is required and how it will be used. Legal opinion suggests that clients who understand the purpose for collecting personal information and agree to disclose it, have provided consent for its qualified use.

In January 2004, PEO published its first privacy policy to its website (www.peo.on.ca). (The original policy has since been updated, expanded and republished.) The introduction to the current policy reads, in part, "the objective of PEO's Privacy Policy is responsible and transparent practices in the management of personal information, in accordance with contemporary privacy expectations. PEO's Privacy Policy also provides guidance as to how it interprets its ability to disclose information 'as may be required in connection with the administration' of the legislation as set out in Section 38 of the *Professional Engineers Act* (PEA)." Section 38 of the PEA states that PEO must keep all of the personal information it holds confidential, unless its regulatory mandate requires disclosure.

PEO's privacy policy outlines how the organization has matched its information gathering processes to the principles outlined in PIPEDA. The policy includes a number of "sub-policies" covering PEO's 38 chapters, Internet privacy, access and correction procedures, privacy safeguards, records retention, the privacy complaints procedure, and the production of a printed privacy brochure.

In September 2004, staff began their privacy policy training in sessions led by PEO's privacy consultants. In addition to learning about information safeguards, employees were required to sign agreements committing them to upholding the new privacy standards. The agreement stipulates that PEO's chief privacy officer will provide training in privacy issues to employees at least once a year. PEO's volunteers are also to be trained in the new policy, and will be required to sign the confidentiality agreements.

Daria Babaie, P.Eng., director of administrative services, said PEO has made a major

commitment to implementing the privacy policy and to ensuring that its procedures, practices, and even its data collection forms, are revised to reflect the new priorities. He added that, in addition to actively seeking employees' input in developing a comprehensive privacy policy, the association is conducting ongoing training to ensure that staff are kept up to date on what is expected of them. Some of that training will include reminding staff to secure their work stations each day, and not to deal with sensitive material at home, or at other unsecured work sites.

He added that because chapters are integral parts of PEO, the privacy policy implementation includes the chapter sub-policy.

Babaie said PEO Council's ratification of Registrar and CEO Kim Allen as chief privacy officer sends a positive message about the association's commitment to privacy issues. "Having the chief privacy officer as the CEO of the organization is an important step in showing members and the public how seriously PEO takes its new privacy policy, and how seriously it will deal with any complaints," Babaie said.

He added that while the privacy policy isn't directly related to PEO's recent emphasis on increasing accountability and transparency to members, it is in keeping with progressive business practices–especially in terms of providing leadership by example in showing compliance with federal (or provincial) legislation.

But PEO is also faced with an additional set of considerations with respect to privacy and its use of personal information. Bruce Matthews, P.Eng., PEO manager of complaints and discipline, says that because of its role as an investigator in matters relating to complaints, discipline and enforcement, PEO requires greater latitude with certain types of personal information. In some cases, this will involve obtaining information about members without their strict consent. In particular, PEO investigators can be expected to be exempted from the information disclosure and consent requirements of either federal or provincial privacy legislation by virtue of section 38 of the PEA. The ability to obtain information through investigation of complaints is believed to override the need to obtain the subject's expressed consent.

Just to be certain, however, PEO, along with the 10 other provincial/territorial engineering regulators, has applied through the Canadian Council of Professional Engineers to Industry Canada for an investigative body designation. One of the conditions of such a designation is that the applicant have a comprehensive privacy policy already in place. Should the investigative body status come through, PEO's regulatory compliance activities would be specifically exempted from PIPEDA.

Fundamental to regulator

"Gathering information of this kind is fundamental to our mandate as a regulator and investigator," Matthews said. He added that PEO has always treated personal information about members with the strictest confidence, especially when conducting investigations or pursuing complaints. The development of the privacy policy, however, will strengthen and standardize the overall process. "One of the really positive things on the safeguarding issue is that the policy will reinforce for all staff the need to keep information strictly internal," Matthews said. "This includes such measures as regarding external email as a non-secure method of communication and therefore making sure that email messages about individuals under investigation don't contain real names or identifiable personal information."

Lawyer Lisa Braverman told *Engineering Dimensions* that there is a clear symbolic value in PEO developing and implementing a policy on the use of personal information. "Engineering firms, as commercial operations, will be covered under PIPEDA legislation," she said. "The question then becomes, how can PEO expect individual engineering firms and practitioners to develop privacy policies if it doesn't have a similar policy of its own?"

Braverman emphasized that while she and Richard Steineke have helped shape PEO's privacy policy, staff and volunteers provided much of the input to tailor the policy to the regulator's particular needs.

"The input and feedback we received from employees and volunteers was significant," she said. "We had originally planned to interview senior staff to assist with the privacy policy development, but we ended up dealing with 32 key personnel, and from there we were able to consult with a good cross section of the entire organization."

Braverman added that PEO appears especially committed to privacy issues compared with some of the other major regulators her firm has been involved with. "PEO appears to be near the top in terms of overall safeguards, but we have to remember that this is a process that isn't expected to be completed all at once. That's why we've established the six-month timeframe to allow the association to implement its policy. It's important to show a transition to an enhanced privacy regime."

The transitional approach to an organization's treatment of personal information is in keeping with the original objectives of the federal government in passing the personal information act.

During a November 19, 2004 presentation to PEO Council, Steineke summarized three main issues underlying the development of PEO's privacy policy–everyone involved with PEO has to be aware that the association has a privacy policy; any staff person or volunteer requesting personal information from a member, applicant or member of the public must explain why the information is being collected; and society now has increased expectations as to how an organization such as PEO will safeguard personal information.

Despite the scope of the project, PEO officials believe the major challenges have already been overcome. Daria Babaie, for example, is optimistic that the March 2005 deadline for full implementation of the privacy policy can be reached. "The project is on schedule at this time and we do not anticipate any major hurdles to completing it on time," he said.

about members with the strictest confidence