PRIVACY LAW

Will privacy patchwork quilt be wedding rings or log cabins design?

By Susan R. Mayer

It is going on three years that Canada has had the *Personal Information Protection and Electronic Documents Act* (PIPEDA), federal legislation protecting personal information in the private sector. Although it does not yet apply to many organizations, come Jan. 1, 2004, PIPEDA will apply to every organization except in certain specific circumstances.

Where an individual handles personal information for only personal or domestic purposes, PIPEDA does not apply to that individual in that regard. So, the family's Christmas card list is safe. And, where an organization handles personal information for only journalistic, artistic or literary purposes, PIPEDA does not apply to that organization in that regard. Paying for groceries will be as entertaining as ever.

But two additional exceptions are significant.

First, where an organization is a government institution to which the federal *Privacy Act* applies, PIPEDA does not apply to that organization.

Second, PIPEDA will not apply to defined intra-provincial activities of some organizations where that province has "substantially similar" legislation. To be substantially similar means to be equal or superior to PIPEDA

Susan Mayer

in the degree and quality of privacy protection offered, says the Privacy Commissioner of Canada (PCC) in his May 2002 Annual Report to Parliament. Once legislation is endorsed as substantially similar by the PCC, a Governor-in-Council order is needed to formalize any exemptions.

Thus, PIPEDA recognizes that there will be patchwork legislation protecting personal information across Canada. The theory is that the provincial legislation will be substantially similar to PIPEDA and, thus, there will be few practical differences regarding compliance requirements.

It's nice in theory. Unfortunately it's not that simple.

For instance, PIPEDA gives no special recognition to organizations that are government institutions under provincial legislation. There is no automatic exclusion of PIPEDA's application where such organizations are already subject to provincial privacy law. These organizations will have to comply with both laws, where the provincial privacy law does not meet the substantially similar test. Complying with both laws will not necessarily be easy — looking at the access provisions usually makes that clear enough.

Then there is the distinction between organizations that are federal works, undertakings or businesses and those that are not. Federal works, undertakings or businesses have had to comply with PIPEDA since 2001. Where a province puts into place private sector privacy legislation, these organizations will likely have to comply with PIPEDA and the new provincial law. A substantially similar exemption may or may not mean that the organization only needs to comply with the provincial law for intra-provincial activities. But these types of organizations likely conduct cross-border activities, which means ensuring compliance with PIPEDA, anyway.

At a practical level, there are bound to be discrepancies with respect to the details of compliance. An organization will likely find itself complying with the higher standard set by combining both laws — or very inefficiently trying to keep track of which standard applies to which activity.

Could the province solve this by offering an exemption so that certain organizations could opt to be subject just to PIPEDA? Not likely, since PIPEDA extends only to commercial activities, whereas the provinces will be able to capture non-commercial activities. The unfairness of that is probably going to get in the way of such an option being offered.

There will also be the inevitable differences between the legislation of one province and the next. Organizations operating in more than one province may be faced with complying with different provincial laws for the same activities in different provinces, and PIPEDA for cross-border activities.

When are these challenges likely to become a reality for organizations? Originally it was thought that the provinces would work to ensure that they each had their own legislation in place no later than Jan. 1, 2004.

As it turns out, most of the provinces are not even attempting to put together their own legislation. So, in 2004, PIPEDA will apply to intra-provincial commercial activities of organizations in those provinces. There won't be two regimes in those provinces, but employees of non-federal works, undertakings or businesses will be left without the personal information protection that PIPEDA offers employees of federal works,

see PROTECTION p.17

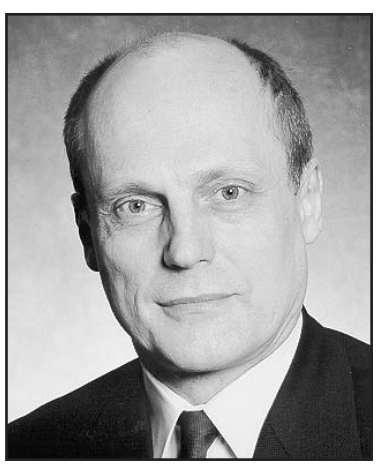
Commissioner says B.C., Alta. bills not 'substantially similar'

By Paul Jones

On April 30 and May 14 respectively, British Columbia and Alberta introduced privacy bills in their legislatures. Bill 38 and 44 are intended to be "substantially similar" to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) so that these provinces can apply to the federal government for a regulation exempting them from the application of PIPEDA to privacy matters entirely within these provinces, as is currently scheduled for Jan. 1, 2004, for provinces that do not have "substantially similar" laws.

However the Privacy Commissioner of Canada promptly sent letters to both provinces advising them of what he described as "very grave deficiencies" that in his view would make it impossible for the government of Canada to recognize the legislation as "substantially similar" to PIPEDA. The letters, dated May 7 and May 27 respectively, may be viewed at *www.privcom.gc.ca*. He has also since given two speeches elaborating on his concerns.

In sending his letters, the Privacy Commissioner may well have initiated a larger discussion about who sets privacy standards in Canada. Many key concepts in privacy law, such as "sensitive information," "implied consent" and "reasonable purposes" (as required by s. 5(3) of PIPEDA) require considerable



Paul Jones

judgment to interpret when organizations wish to apply them to specific facts. The Privacy Commissioner has often said in his speeches that for the purposes of PIPEDA, he is the mythical "reasonable person." It follows that he believes that he will set the standards for the interpretation of key privacy concepts. The question now is whether the judges and the federal government will agree with him.

PIPEDA has an unusual structure that makes it more difficult to interpret. The substantive provisions are set out in the CSA Model Code appended to the Act as a schedule. To correct this problem, B.C. and Alberta wrote the privacy principles in the CSA Model Code into their legislation. B.C. managed to do this in 33 pages compared to the 120 pages that were needed by Ontario for the draft *Privacy of Personal Information Act, 2002* that was aborted by the Ontario Cabinet last year.

B.C. and Alberta also benefited from the experiences to date with PIPEDA and included items to clarify what is "work product information" or "contact information" (and therefore not personal information). There are provisions for the transfer of personal information that is incidental to the sale of the assets of a business. Alberta has gone even further and exempted the non-commercial activities of non-profit organizations from the application of Bill 44.

The Privacy Commissioner has objected to a number of these attempts to resolve existing

see COMMISSIONER p.18

Balance between personal privacy and collective security remains elusive

By Jennifer Fiddian-Green

Do you have family overseas? Whose business is it if you send or receive money from them? How often do you make large dollar transfers between your accounts?

In Canada we are accustomed to a significant level of privacy concerning our personal financial information. This will be reinforced in January 2004, when Canada's privacy law for the private sector, the *Personal Information Protection and Electronic Documents Act (*PIPEDA*)* will apply to all personal information collected, used or disclosed in the course of commercial activities by all private sector organizations.

Under PIPEDA, an individual's personal information is only to be collected, disclosed or used with the individual's knowledge and consent. With ever-increasing electronic connectivity, protecting our right to privacy is more important than ever before. There is constant pressure to sacrifice personal privacy in the interest of collective security from crime and terrorism.

Canadian financial institutions and other types of businesses, including real estate brokers and dealers, insurance brokers, money transmitters — and in some cases your accountant — are required to report to a new agency, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). FINTRAC was created by Canada's *Proceeds of Crime (Money Laundering) & Terrorist Financing Act* (PCMLTFA). Any transactions suspected of being money laundering and/or terrorist financing must be reported. These reports are made without the individual's knowledge or consent and must be kept confidential. Communication of a report is known as "tipping off" and is not allowed.

If staff members at a local bank have reason to believe that a transaction is suspicious, they are required to report it to their supervisors. If their supervisors agree, it is likely that FINTRAC will receive a suspicious transaction report within 30 days of the characterization of a transaction as suspicious.

How close to home is this? My husband and I recently purchased our first home. We chose to deal with an Internet bank, President's Choice Financial.

see REPORTING p.18

PRIVACY LAW

Organizations are caught between two contradictory statutes

REPORTING

–continued from page 16–

We pay no fees and enjoy higher savings interest rates. For our deposit payment and the funds paid at closing, we had to wire transfer funds from our Internet bank to a bank we could physically visit in order to obtain certified cheques. The staff at the local branch had no idea who we were, where our money came from or what we were doing. There is a good chance the staff member with whom we dealt reported the situation to her supervisor as suspicious.

In another case, a friend of ours who is a Canadian citizen of Iranian descent recently ventured off on a United Nations peace-building mission in Afghanistan. Her movements of funds — taking money with her when she travelled and having funds sent to her while she is overseas — are under scrutiny.

The organizations required to make reports of suspicious transactions are all required to have a comprehensive due diligence program to demonstrate compliance with the PCMLTFA. The penalties can be high if they do not — including jail terms and millions of dollars of fines. Many of the organizations I have had the opportunity to work with maintain a list of high-risk countries. Transactions to and from these countries are flagged for review. How much does an organization need to know, or not know as the case may be, to be suspicious of terrorist financing?

The Charter of Rights gives each citizen the right to be secure against unreasonable search or seizure. As a consequence of this protection, a justice of the peace will only issue a search warrant provided certain criteria are met. These criteria include having reasonable and probable grounds to believe that something will be found in respect of an offence against a law.

Consistently, the PCMLTFA also requires transactions to be reported only when there are reasonable grounds to suspect that the transaction is related to the commission of a money-laundering offence or financing of terrorist activity. The difference today is that the decision about what constitutes reasonable and probable grounds is now being made, not only by justices of the peace in the case of search warrants, but as well by individual compliance officers of businesses all across the country for transaction reporting to FINTRAC.

FINTRAC is an independent federal agency responsible for the collection, analysis, assessment and disclosure of information.

Jennifer Fiddian-Green

Information about suspected money laundering or terrorist financing activities may be disclosed to police authorities, to the Canadian Security Intelligence Service (CSIS), to the Department of Immigration and to the CCRA.

FINTRAC is subject to the PIPEDA like all other federal organizations and must take care not to abuse personal information. The PCMLTFA specifically provides that FINTRAC can only disclose information to police where there are *reasonable grounds* to suspect that the information would be relevant to investigating or prosecuting a money laundering or terrorist activity financing offence.

It's interesting to note that the information may not always get communicated as one would expect. Let's consider the following scenario: A local bank employee reports a specific transaction as suspicious — one that we would all agree involves reasonable and probable grounds of suspected money laundering. This transaction is subsequently reported to FINTRAC.

After assessment of the report, FINTRAC determines that there are reasonable and probable grounds to disclose the information to law enforcement. Only "designated information" as defined in the Act and regulations can be disclosed. This designated information, in the words of one federal law enforcement officer I recently spoke to, "is not enough to do anything with unless we already have an investigation underway." It is very important to have strict controls on the information once collected, but our security is best served by using the information proactively. A positive impact of this legislation is that FINTRAC becomes a convenient one-stop source of intelligence for law enforcement.

What the PCMLTFA demands will undoubtedly enhance law enforcement investigations. Reports to FINTRAC are intended to link information from across industries and institutions and to proactively target law enforcement investigations. However, there are risks, one of which is law enforcement's relationships with financial institutions. Anecdotal information reveals that in some areas police agencies that received suspicious transaction reports in the past are now no longer receiving them directly.

As organizations meet the challenge of implementing their reporting regimes and of protecting the privacy of their customers, making the distinction between filing a report to law enforcement (voluntary) and one with FINTRAC (mandatory) perhaps becomes a question of choosing how many agencies to deal with. It remains to be seen if law enforcement is frustrated as reports are filtered through FINTRAC or if there truly is an overall benefit to our collective personal security. FINTRAC, a relatively new federal agency, needs time to make its mark in the fight against money laundering and terrorist financing.

So whose business is it when you transfer money to family overseas or among your own personal accounts? Not just yours anymore. Our system here in Canada requires those who facilitate transactions for us to make reports if they have reason to be suspicious of money laundering or terrorist financing activities.

The pendulum is swinging further away from the protection of personal privacy than we might all like, but swift responses to legitimate terrorist and money laundering activities are essential. Our intelligence and protection agencies need all the help they can justly obtain.

Financial institutions and other organizations required to report under the PCMLTFA are caught answering to these two very demanding contradictory pieces of legislation: reporting vs. protecting privacy. The choices made today will be scrutinized tomorrow and require our continued vigilance.

Jennifer Fiddian-Green, CA•IFA, CMA, CFI, CAMS is an investigative forensic accountant and a certified anti-money-laundering specialist with Grant Thornton LLP.

Who really decides national privacy standards?

COMMISSIONER

–continued from page 16–

problems with PIPEDA. In order to solve the problem of how to handle existing databases, B.C. and Alberta included provisions that did not invalidate databases collected before the adoption of privacy legislation, and allowed the continued use and disclosure of such databases provided that such actions were within the scope of the original purposes.

The Privacy Commissioner has attacked this restriction as illusory because there is likely no evidence as to the original purposes. However as the judge found in *Thomas v. Robinson*, 34 C.C.L.I. (3d) 75 (Ont. S.C.J.), reasonable purposes can be inferred from the context in which the information was collected.

The Privacy Commissioner also objected to B.C. specification as to what constituted implied consent and when opt-out consent may be used. He considers "implied consent" to be a weak form of consent that is acceptable only in limited circumstances, and inferred that, because Bill 38 did not specifically mention "explicit consent," some organizations would rely only on implicit consent.

However in PIPEDA Case Summary #153 issued April 14, 2003, the Privacy Commissioner found that it was acceptable for a telecommunications company to expand its use of previously collected workload statistics to manage the performance of individual employees. The new purpose was considered reasonable, the company took appropriate measures to inform the employees of the new purposes, and that performance evaluation "…, an integral part of the employer-employee relationship, is a condition of employment to which the complainants gave implicit consent when they agreed to work for the company."

The Privacy Commissioner also objected strongly to the provisions allowing the collection of employee personal information without consent if the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship, and the organization notifies the employee of the purpose and the collection in advance — even though he had rendered such a decision less than a month earlier.

Shortly after assuming the post, the Privacy Commissioner announced that in his opinion for a law to be "substantially similar" to PIPEDA, it must provide equal or superior privacy protection. In response the federal government published a description of the process that it will use to make such a determination in the *Canada Gazette*. The description included a quote saying "We are really looking for similar principles … We are not trying to prescribe in detail what provinces need to do." Both B.C. and Alberta consulted with the federal government during the drafting of their Bills.

There were also objections regarding the access provisions, the expanded scope of the concept of "investigation," and in the case of Alberta, to the scope of the power to make regulations, its provisions on access fees, and the exemptions for professional regulatory bodies and non-profit organizations. The Privacy Commissioner says that the Bills restrict access where a third party is providing information or opinions about the individual. Such restrictions would not be in accord with the comments of the Supreme Court in *Lavigne v. Canada*, 2002 SCC 53.

On May 13 the Federal Court Trial Division released its decision in *Diane L'Écuyer c. Aéroports de Montréal*, 2003 CFPI 573, in which it reviewed the decision of the Privacy Commissioner in PIPEDA Case Summary #20, where he held that there was no implied consent. The court strongly disagreed.

The response of the federal government to the applications of B.C. and Alberta for exemptions from PIPEDA may well clarify how to reasonably interpret the provisions of PIPEDA and the findings of the Privacy Commissioner.

Although originally from British Columbia, Paul Jones practises privacy, franchising and distribution, intellectual property and competition law in the Toronto office of Miller Thomson LLP.

Government's attitude seen as key problem

FOI

–continued from page 7–

Alan Leadbeater, an administrative law lawyer who has been deputy information commissioner since 1991, told *The Lawyers Weekly* the courts' decisions last year simply reflected the strong principles and philosophy of the statute they were interpreting.

"I don't think there is a philosophy on the part of the courts to 'get' the government, or to support the Information Commissioner," he observed. Leadbeater suggested that the public's right to access and accountability ultimately depends much more on the government's attitudes than on the Act itself.

"That, to a certain extent, is why it's so important at the federal level to have the courts available because seemingly we are stuck with a milieu where we don't have strong leadership support — we didn't from the Conservative government that was in power when the Act came into force, and all governments since. It just seems that there is such a deep culture … here of desire to control information that there just is no real meaningful embrace of the idea of transparency," said Leadbeater. Until the government's attitude changes, he predicted that the courts "will be called upon ... to ... referee some of these differences of view between the Commissioner and the government."