

Personally Yours

PRIVACY LAW SECTION / SECTION DU DROIT DE LA PROTECTION À LA VIE PRIVÉE

Volume 3, No. 1
September / septembre
2002

In this Issue:

Bank-Related Website Reports
under PIPEDA re. Access,
Collection and Disclosure

Message from the Chair

Anti-terrorism initiatives
erode privacy

Federal Court Allows IMS
Health Case to Proceed

"Substantially Similar"
Applied

Non-Statutory Restrictions on
the Use of Personal
Information

Bank-Related Website Reports under PIPEDA re. Access, Collection, and Disclosure

*Karen Spector**

The *Personal Information Protection and Electronic Documents Act*¹ ("PIPEDA") requires the Privacy Commissioner of Canada (the "Commissioner") to prepare a report within one year after a complaint is filed or is initiated by the Commissioner². The report is to contain the Commissioner's findings and recommendations and any settlement that was reached by the parties³, among other things.

PIPEDA requires the Commissioner to send the report to the complainant and to the organization without delay⁴. However, there is no statutory requirement that the Commissioner publish the report or otherwise make it available to the public. Further, PIPEDA authorizes the Commissioner to make public any information relating to the personal information practices of an organization if the Commissioner considers that it is in the public interest to do so⁵.

The Commissioner appears to have adopted the following practice with respect to reports:

- The Commissioner posts certain reports on his website, at www.privcom.gc.ca, for "educational purposes", if he thinks that they are "indicative of how PIPEDA is working"⁶.
- The posted reports are an anonymized summary of the original reports.

- At the Commissioner's discretion, fuller text versions of certain reports may be published. For example, in February 2002, the Commissioner released his full report regarding a request for a credit score⁷ and in March 2002, the Commissioner released his letter to Air Canada's Manager of Privacy Compliance "due to the public and media interest"⁸.

Website Reports

Since January 1, 2001, PIPEDA has applied to personal information that banks collect, use or disclose in the course of commercial activities. Not surprisingly, 30 of the Commissioner's 61⁹ website reports relate to banks.

This article focuses on reports¹⁰ flowing from complaints about three types of personal information management practices, which account for approximately 80 per cent of the reports:

1. Failure or refusal to provide access to personal information
2. Improper collection of personal information
3. Disclosure of personal information without the individual's knowledge or consent



Failure or refusal to provide access

The complaints were made by customers, employees and an estate executor who requested access to personal information including:

- a bank-generated credit score,
- codes from a credit reporting agency that the complainant was not able to understand;
- an employment file that referred to third parties
- a signature card for a safety deposit box
- a tape recording of a telephone conversation between the complainant and a bank director

The Commissioner's investigations revealed that in some cases, the personal information was not or no longer in the bank's custody or control because the bank had lost it, destroyed it, or never had it in its possession. In other cases, despite being in possession of the personal information, the bank failed to meet statutory deadlines¹¹ because its access policies pre-dated PIPEDA or the bank could not locate the access request.

The Commissioner found that PIPEDA required banks to provide access to personal information for these reasons, among others:

- Disclosures required by PIPEDA constitute disclosures authorized by law, for the purposes of an exception in a non-disclosure agreement; and
- PIPEDA does not absolve a bank from compliance on the grounds that it would incur significant expenses for training and certifying bank employees or that the individual could obtain the same personal information elsewhere.

In one situation, the Commissioner found that a credit score generated by a bank constituted personal information. Nevertheless, he supported the bank's reliance on PIPEDA's confidential commercial information exemption¹². The Commissioner solidified his position, when, five months later, he released a report stating that customized credit scoring models internal to financial institutions should in future be deemed confidential commercial information for purposes of PIPEDA.

According to the website reports, a well-founded complaint could be considered to be "resolved" when the complainant was satisfied that the bank had provided the personal information requested. A former em-

ployee, who had been dismissed for harassment, requested a copy of his employment file from a bank. The Commissioner determined that the bank could not rely on exemptions relating to third-party information¹³ and threats to the life or security of other individuals¹⁴ as the basis for denying access. Nevertheless, because the complainant was satisfied when the bank provided him with a typed copy of anonymized comments made about him rather than the employment file he had requested, the Commissioner found that the matter was resolved.

The Commissioner recommended that the banks correct their personal information management practices by, among other things:

- Collaborating with credit reporting agencies in developing "understandable", "consumer-friendly" formats for credit reporting information; and
- Revising or developing written policies and practices regarding access, retention and destruction.

Improper collection of personal information

Based on his investigations, the Commissioner found that:

1. A customer who complained that the bank had tape-recorded telephone conversations without his consent, had in fact given his express consent to the collection when he signed an agreement in which the bank detailed its practice of tape-recording telephone banking transactions.
2. A bank that had provided two different purposes for its mandatory collection of an account applicant's birth date, had no legal requirement to collect birth dates, and had made no effort to document or identify any purposes for collecting personal information from account applicants.
3. A bank that required established customers to produce identification to bank tellers before making withdrawals, at a certain branch that had implemented a fraud prevention program, was able to show that it had adequately identified the purpose of the collection, safeguarded customers' personal information in the hands of the bank's junior officers (tellers), and that a reasonable person would have considered the collection appropriate in the circumstances.

4. A bank that demanded authorization to conduct a credit check as a condition of opening an account, with no credit privileges, for the purpose of protecting against identity theft and reducing fraud was not able to show that a credit check would achieve this purpose, was required by law, or would be reasonable under the circumstances.

The Commissioner recommended that banks:

- Cease collecting birth dates as a mandatory condition for the opening of accounts until such collection is required by law¹⁵;
- Identify and document the purposes for which they collect personal information;
- Implement measures to specify the purposes to individuals, at or before the collection; and
- Train operators who take account applications by telephone.

Disclosure of personal information without the individual's knowledge or consent

Three separate complaints dealt with disclosures of personal information by banks to third parties including a collection agency, a private market research firm, and the customer's employer. The Commissioner found that a bank:

- May disclose personal information without the individual's knowledge or consent for the purpose of collecting a debt¹⁶ and that the information transfer was a consistent use to which the debtor-complainant had consented through the cardholder agreement;
- May disclose a customer's personal information to a third party without the customer's consent where,
 - it has provided the customer with written notice of its practices regarding personal information at the time she opened her account,
 - the disclosure is consistent with the stated practices,
 - the information had been limited by a confidentiality agreement, not sold and duly destroyed after use.
- May not disclose a customer's personal information to a third party with whom the bank has a confidentiality agreement, if the third party subsequently discloses the personal information to another

party whose collection, use and disclosure of the personal information is not provided for in the confidentiality agreement.

- May not, as a "business courtesy", disclose a customer's rude and inappropriate conduct at the bank to his employer because a reasonable person would not under any circumstances expect his bank manager to make such disclosures to his employer.
- May not disclose that a client is a bankrupt in the address window of her bank statement.
- May imply the consent of the person cashing a cheque to record his or her account number on the back of the cheque, even though it may be disclosed to the third party who wrote the cheque, since it is a reasonable practice and it is reasonable for a customer to expect such a practice.

Conclusion

Based on these website reports, PIPEDA, as interpreted and applied by the Commissioner, requires a bank:

- To provide access to personal information in an understandable format within the statutory deadline;
- To comply with PIPEDA's access provisions regardless of the expense;
- To revise or develop document retention and destruction policies;
- To collect personal identifiers, such as birth dates, only when it is authorized or required by law;
- To implement measures for specifying the purposes for which they collect information, including training staff; and
- To disclose an individual's personal information in a manner consistent with its stated practices, the terms of a confidentiality agreement, or with the consent of the individual.

Finally, a bank's collection, use, and disclosure of personal information will be measured against what a reasonable person would consider appropriate in the circumstances.

* *Karen Spector, Barrister & Solicitor, (416) 482-6642, KASprivacy@rogers.com*

¹ S.C. c-5

² Subsection 13 (1)

³ clauses 13 (1) (a) through (d)

⁴ Subsection 13 (3)

⁵ Subsection 20 (2)

⁶ I had incorrectly assumed that the “Findings of 2001” and the “Findings of 2002” posted on the Commissioner’s website were comprehensive listings. On July 17, 2002, when I could not locate a particular report that I had read about in the newspaper on the website, I telephoned the Commissioner’s office. I learned from an inquiry officer that only certain “educational” reports are posted.

⁷ News release, February 27, 2002

⁸ News release, March 20, 2002

⁹ Based on website listings, as at August 23, 2002

¹⁰ This article is based exclusively on the publicly-available website reports and not on the original, full-text reports.

¹¹ Subsection 8(3)

¹² Subsection 9(3)(b)

¹³ Subsection 9(1)

¹⁴ Subsection 9(3)

¹⁵ Refer to the most recent *Proceeds of Crime (Money Laundering) Regulations* or other relevant legislation for requirements.

¹⁶ subsection 7(3)(b)

Message from the Chair

Does Electronic Access to Personal Information Diminish Privacy When Compared to Publicly Available Paper Records?

*Priscilla Platt**

There are few areas of modern life that afford perfect privacy; this is particularly true with the advent of technology. For example, recently it was reported that the B.C. Supreme Court “may soon stop publishing family law cases on its website, essentially because of privacy concerns.” [Lawyers’ Weekly, May 24, 2002, at 3, in an article written by Gary Oakes, from Victoria] It was reported that the Court had received complaints about the ease with which members of the public could access this sensitive information. Nonetheless, it was noted that this possible change would not affect access to these judgments, in paper and electronic formats through legal publishers and at court registries. [Ibid.]

On May 10, 2002, the Divisional Court, in a case that has been reported as *Gombu v. Ontario (Assistant Information and Privacy Commissioner)*, had occasion to consider this issue ([2002] O.J.No. 1776). The record requested from the City of Toronto under the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* was an electronic database of campaign contribution records for the municipal election in 1997. Under the *Municipal Elections Act* (the MEA), paper records of this information are required to be made available publicly. However, as thousands of pieces of paper were involved, the requester, for ease

of reference, sought the electronic record kept by the Clerk. The City had claimed that the electronic version of the information was personal information that was not available to the public and was therefore not capable of being released under MFIPPA since to do so would breach the privacy of the individuals involved.

The Information and Privacy Commissioner/Ontario (IPC), in Order MO-1366, agreed with the City and upheld the privacy exemption for the electronic record. In so doing, the IPC found that the electronic record was not maintained as a public record and that “the disclosure of the personal information in electronic form, where it can be massively disseminated, matched and merged, and used for purposes far beyond those for which the information was collected in the first place, is a relevant factor to consider, and weighs significantly in favour of non-disclosure of the personal information in that format. [at 15]

In a Postscript to the ruling, the Assistant Commissioner, Tom Mitchinson, stated that

Finding the appropriate balance between the right of access to government-held information and

the right to personal privacy is seldom more complex than when faced with requests for publicly available personal information in electronic format. (at 18)

On judicial review undertaken by the requester, McCombs J., for the Court, set aside the IPC's decision and ordered the electronic database to be disclosed. While the Court found that the electronic database was prepared to carry out the mandate of the MEA [at para.16], and was therefore publicly available, it went on to find that the analysis regarding the distinction between paper records and their electronic counterparts flawed. McCombs J. stated that

In my opinion, the view taken by the Commissioner of the dangers of misuse of the database is not reasonable, particularly in the context of the present electronic age in which governments

are increasingly moving to electronic information-storing... Moreover, any danger of misuse exists even with the paper version presently available to the public. In today's electronic age, the paper version can be converted to electronic form by use of an electronic "scanner". Once thus converted, the danger of inappropriate use of material remains. [at para.26]

The Court also noted that full disclosure of the electronic database would, in this context, "achieve the important objective of enhancing the transparency of the political process..." [at para. 28] It was reported that the IPC is seeking leave to appeal the Divisional Court's decision to the Court of Appeal. [The Toronto Star, "Privacy Office Appealing Database Release", May 28, 2002]

* Priscilla Platt, Chair, Privacy Law Section.

Anti-terrorism initiatives erode privacy

John Z. Swaigen*

New laws and changes in security procedures throughout the world since the September 11 suicide bombings have authorized numerous new forms of intrusion on privacy in the name of combating terrorism.. Both democratic countries like Canada, the United States, Britain and Australia, and less democratic countries such as South Korea have introduced laws that reduce human rights and civil liberties to increase security and public safety.

This article will outline some of the initiatives in Canada and the United States. It is by no means complete, nor have we necessarily seen the end of new initiatives. In our November 2001 issue, we reported that the Canadian Government had introduced Bill C-36, the *Anti-Terrorist Act*. Among other privacy-intrusive measures in this Bill, it removed from the ambit of the federal *Privacy Act*, *Access to Information Act*, and *Personal Information Protection and Electronic Documents Act*, information that is the subject of secrecy certificates that the Attorney General of Canada may issue.

Following criticism by the federal Privacy Commissioner, George Radwanski, the federal Information Commissioner, John Reid, and others, the government amended the bill to reduce the impact of these certificates on the federal access and privacy laws. A certificate will still prevent an individual from obtaining access to or correcting his or her personal information, but it will no longer override provisions of the *Privacy Act* and PIPEDA protecting privacy in relation to the collection, use, and disclosure of personal information.

Other provisions in the *Anti-Terrorist Act* that affect privacy include broader police and security agency powers to intercept private communications, the power of police to detain terrorism suspects without trial, the authority to compel testimony before a court in "investigative hearings", and greater access by several categories of government officials to a variety of personal information. These access powers include broader powers to take DNA samples from suspected terrorists and increased authority for law enforcement officials to obtain information from individuals' government income tax files.

In December 2001, the Canadian Government passed Bill C-44, an Act to amend the Aeronautics Act. This Act permits airlines operating in Canada to give designated agencies in other designated countries a variety of personal information about airline passengers and crew members flying into those countries, overriding privacy provisions in PIPEDA. A regulation has since been promulgated that designates the United States as a country that may receive this information, and sets out the kind of information that may be provided. It includes passenger names, dates of birth, citizenship, gender, passport or visa numbers, whether a passenger had a prior reservation, travel agency, the date the ticket was issued, the passenger's itinerary, and whether the ticket is one-way or a return ticket.

Bill C-55, the *Public Safety Act*, was introduced by the federal government on April 29, 2002. It had not been passed when the House of Commons rose for its summer break.

Bill C-55 amends 21 existing statutes. The Bill attracted criticism from the federal Privacy Commissioner because it provides authority for the RCMP and CSIS to obtain a wide variety of personal information about airline passengers from air carriers and ticket agencies and to data match it in ways that go beyond preventing or detecting terrorism. For example, this information can be used to execute arrest warrants issued under the Criminal Code for some indictable offences that are unrelated to terrorism. (Falsely branding cattle is one offence identified by the Privacy Commissioner). Also, much of this information may be permanently recorded through "data summaries" even though the legislation requires the original document to be destroyed within a few days if it is not useful for the purposes for which it was collected.

Bill C-55 also potentially permits export controls, which could affect sale of encryption programs, which are privacy tools. In addition, the Minister of National Defence can order widespread computer surveillance to intercept communications to or from government computer systems for the purpose of identifying or preventing unauthorized use, interference, or damage to computer systems or networks or the data they contain — all without obtaining a warrant.

The bill provides authority for more airport screening. Screening is defined to include searches of individuals, luggage, carry-ons and vehicles by any manner authorized by regulations, security measures or emergency directions made under the *Aeronautics Act*. Although specific techniques and technologies are not mentioned, concerns have been raised that this may include machines that "see" through clothing and biometrics.

In May of this year, federal Justice Minister Martin Cauchon announced that, this fall, Canada will introduce legislation designed to implement parts of the international Cybercrime Treaty, which Canada has signed, but not yet ratified.

The legislation will give police wider access to the electronic information held by Canadian telephone companies, banks and Internet Service Providers ("ISPs"). Police will have authority to require firms to preserve billing information and email trails and provide them to police on demand. Currently, police can obtain a warrant to seize existing information where there are grounds to believe they will provide evidence of a crime, but police cannot require companies to save or continue collecting information until they can obtain a warrant.

At the provincial level, legislatures have also introduced bills that shift the balance between protecting privacy and achieving security. Ontario amended the *Vital Statistics Act* to make it more difficult to obtain false birth certificates, marriage certificates, and death certificates — a measure to prevent "identity theft" which is privacy protective. However, in order to verify the identity of applicants and holders of such documents, government officials are given greater power to collect personal information about them and share it among different agencies.

In May 2002, the Alberta government introduced the *Security Management Statutes Amendment Act*, which amends seventeen statutes. It contains provisions similar to Ontario's changes to the *Vital Statistics Act*. It also contains several provisions that increase the authority of government officials to collect personal information and that permit agencies to share this information with each other. The officials given broader powers to collect and share information include police, government departments, motor vehicle registrars, medical officers of health and nurses. The United States has been particularly active, both

at the federal and state levels, with several states introducing legislation that mirrors initiatives passed federally. The first federal initiative to pass was the *USA Patriot Act*, signed into law by President Bush on October 26, 2001.

Along with other measures affecting privacy, it extends reporting requirements in money-laundering legislation to cover terrorist financing and permits intelligence agencies to intercept communications to and from citizens and permanent residents. It also expands the duration of wiretap warrants and the length of delay in notifying targets after the wiretap has ended; the power of police to require DNA samples; the ability of both law enforcement agencies and intelligence agencies to share information; and “sneak and peak” warrants (warrants that permit search of premises without the occupant’s knowledge).

The *Aviation and Transportation Security Act* became law on November 19, 2001. The Act requires screening of all passengers and inspecting all checked and carry-on luggage for weapons and explosives immediately “by all possible means”. This could include X-ray machines, dogs, hand-search, and where there are insufficient personnel or machines to search each bag, by matching boarded passengers to checked luggage (i.e., if the passenger hasn’t boarded, the luggage can’t be loaded on the plane). The law provided that by the end of 2002, all checked baggage must be checked for explosives by machines capable of detecting explosives. However, these requirements have since been relaxed.

Initial attempts to use facial scanning devices at airports to match the faces of passengers to images of suspected terrorists stored in a database have failed. Tests at two US airports resulted in numerous false positives, operator exhaustion, and false negatives when a passenger tilts his or her head at certain angles or dons eyeglasses.

The law also requires airlines to use video monitors or other devices to alert pilots in the cockpit to suspicious activities in the cabin and at least one aircraft manufacturer has begun to install such cameras in its new airplanes.

On the other hand, proposals in the United States and Britain to install video cameras that will monitor the activities of pilots have met resistance from the pilots, who claim this will violate their privacy.

Various proposals have been put forward to create a national identity card and to modify existing identity card systems. One initiative that has found favour with President Bush is a proposal to create unified national standards for drivers’ licences, with the possible inclusion of biometric identifiers on the licence cards. Another initiative by a national airline industry is a proposal for a “voluntary” national passenger identity card as a way of enhancing security at airports. Those who choose to use the card would be subject to less screening, and thus get faster service at airports.

The *Cyber Security Enhancement Act* passed the House of Representatives on July 15, 2001 by a vote of 385-3. The Senate is expected to pass the bill easily when it resumes sitting in October. The Bill has attracted criticism from human rights and civil liberties associations because it will make it easier for government agencies to obtain electronic communications without a warrant or probable cause to believe a crime has been committed.

Stored communications like email and voicemail will be available to any government entity (not just law enforcement agencies) if it can convince a service provider that releasing the information is necessary to prevent “death or serious physical injury”. There is no requirement to obtain a warrant or other judicial authorization. Previously, service providers were not permitted to give out this information without a court order.

ISPs will be required to store electronic records such as customer emails for at least 90 days or face penalties.

The Bill would allow limited surveillance of computer usage without a court order when there is an “ongoing attack” on an Internet-connected computer or “an immediate threat to a national security interest”. The surveillance would be limited to obtaining a suspect’s telephone number, IP address, URLs or email header information — not the contents of the online communications or telephone calls.

Two bills entitled the *Homeland Security Act* that are very similar to each other were introduced in the House of Representatives and the Senate in July 2002. The Bills would create a new Department of Homeland Security that will likely absorb the Coast Guard, the Customs Service, the Secret Service, part of the

Immigration and Naturalization Services, and the Federal Emergency Management Agency. Both bills would leave the FBI and CIA untouched, except for the transfer of the FBI's National Infrastructure Protection Center.

On their face, the bills do not provide this department with any new intelligence collection authority, but many of the components being transferred have intelligence divisions and will carry their investigative and intelligence authority with them.

In July, the Justice Department also announced its intention to create "Operation TIPS", the Terrorism Information and Prevention System. The Depart-

ment would recruit one million volunteers from occupations such as letter carriers, truckers, and utility workers. They would be encouraged to report any suspicious behaviour.

However, it is questionable whether this network of informants will be established, since House leaders as well as the media and civil liberties groups have suggested that recruiting citizens to spy on their neighbours, as the East German Stasi police did at the height of the cold war, may not be completely consistent with American values.

* *John Z. Swaigen, Information & Privacy Commission/ Ontario, (416) 326-3920, jswaigen@ipc.on.ca*

Federal Court Allows IMS Health Case to Proceed

*Barbara McIsaac**

In a decision issued May 6, 2002 Prothonotary Hargrave of the Federal Court refused a motion by IMS Health Canada to strike an Application for Judicial Review, which had been brought against it by Ronald Maheu. Maheu had brought the Application before the Federal Court pursuant to the provisions of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") after a finding by the Federal Privacy Commissioner that a database maintained by IMS Health regarding the prescribing habits of physicians did not constitute a database of personal information within the meaning of PIPEDA. The Privacy Commissioner's view was that such information regarding the prescribing habits of the physicians constituted work product or work related information rather than personal information.

Maheu, who is not a physician, but appears to be a competitor of IMS Health who has been involved in a number of litigious matters with IMS Health, applied to the Federal Court for a ruling that IMS Health was violating PIPEDA by continuing to collect and compile such information.

IMS Health brought a motion seeking, first, to strike out the Notice of Application for Judicial Review as an abuse of process. Alternatively IMS Health was seeking to require Mr. Maheu to post security for costs on the basis that he is impecunious and that the proceeding is frivolous and vexatious.

The Prothonotary found that the material which had been filed on the motion did appear to indicate that there was reason to believe that the proceeding was frivolous and vexatious in the sense that it was not brought as a fair and honest use of the process of the court in order to extend the PIPEDA, but rather for what is arguably and improper purpose, that of obtaining a commercial advantage. However, the Prothonotary found that the standard for striking an Application is very high and that, given the early days of the PIPEDA legislation and the fact that there was, to date, no judicial interpretation of its meaning or the extent of its intended judicial review provisions, he was not prepared to strike the Application. He did, however, find that IMS Health had clearly established that it appeared to be reason to believe that the proceeding was in fact frivolous and vexatious and that Mr. Maheu would not have sufficient assets in Canada available to pay any costs, which might be awarded, to the respondent IMS Health. Accordingly, he found that it was appropriate to order security for costs and he did order security for costs be posted in the amount of \$12,000.00.

Barbara McIsaac, McCarthy Tétrault LLP, (613) 238-2105, bmcisaac@mccarthy.ca

“Substantially Similar” Applied

The Privacy Commissioner of Canada and Quebec’s Personal Information Regime

Jeffrey Kaufman and Daniel Fabiano*

As previously discussed in *Personally Yours*, Canada’s *Personal Information Protection and Electronic Documents Act*¹ (*PIPED Act*) was intended to set a national standard against which the provinces could shape their own methods for regulating personal information management. As provincial frameworks for privacy protection develop, there will no doubt be variation to account for regional concerns or preferences. The recent Annual Report by the Canadian Privacy Commissioner, George Radwanski, is in many ways a barometer for the sorts of provincial deviation from the federal norm that will be tolerated by his office. By examining the Commissioner’s analysis of the Quebec legislation, *An Act Respecting the Protection of Personal Information in the Private Sector*,² some insight can be gleaned as to how other provinces can contour their own laws so as to be substantially similar to the *PIPED Act*.

Working Definition

Industry Canada and the Privacy Commissioner both assert that to be considered substantially similar, any provincial legislation will have to contain, at a minimum, the ten principles set forth in Schedule 1 to the *PIPED Act*. While all ten principles are interrelated, particular emphasis is placed on access and correction rights, the means of oversight and redress, a reasonable person test for consent to use personal information, and on the requirement of consent itself. As the Commissioner writes, “In assessing provincial legislation, I will interpret substantially similar to mean equal or superior to the *PIPED Act* in the degree and quality of privacy protection provided. The federal law is the threshold or floor. A provincial privacy law must be at least as good, or it is not substantially similar.”³

In his report, the Privacy Commissioner takes each of the emphasized points and attempts to draw out similarities between the Quebec legislation and the

federal standard. In particular his discussions of oversight and redress, a reasonable person test, consent, and his brief mention of openness and accountability, merit comment for their precedential value.

Oversight and Redress

Generally, the principles of oversight and redress encompass the complaint and resolution process. Individuals must have the ability to complain of privacy violations to a fully independent oversight body, with a mandate to investigate, mediate, and resolve complaints, make recommendations, and issue orders. Such a body must have a full range of investigatory powers, including the ability to seize documents, enter premises, compel testimony, and initiate audits of an organization’s practices. The Commissioner finds that the Quebec law forges a strong oversight role for the province’s Privacy Commission that is at least equal to its federal counterpart.

This finding of similarity is accomplished despite the fact that the actual mechanisms of oversight and redress vary considerably. The *PIPED Act* allows a complainant or the Privacy Commissioner, after reporting on the complaint, to apply for a hearing in the Federal Court of Canada to order an organization to correct its practices or to pay damages. Of note is the aid that the Commissioner can lend to complainants throughout the court process. Though the federal Privacy Commission is an investigative body, in Quebec, the Commission is both investigative and adjudicative. The Quebec Commission can make any order it considers appropriate to protect the rights of the parties, and can rule on any issue of fact or law. Indeed, the Quebec Commission’s role is to both police and judge breaches of privacy.

In determining whether the Quebec provisions are substantially similar, the Privacy Commissioner notes that any comparison is difficult. Beyond the structure

of the Commission, the Quebec legislation has a unique context, as it builds on the privacy protection found in the Quebec *Civil Code* and the *Quebec Charter of Human Rights and Freedoms*. Articles 35 to 41 of the *Civil Code* deal specifically with privacy protection. Given these added layers, wronged individuals have the option to seek redress and damages under the *Civil Code* or the private sector legislation — with the associated advantages and disadvantages of each.

The expansive powers of the Quebec Commission, coupled with the provisions in the Civil Code, are different from the structure laid out in the *PIPED Act*. Still, a privacy regime need not be encompassed in one act; in assessing whether a province has a substantially similar privacy regime, regard must be had for all of the elements of a provincial system. The concern is whether the redress provisions are adequate in substance, the actual mechanisms of redress are secondary, and indeed can take many forms. The Privacy Commissioner has determined that so long as there are parallel fines for contravention, and recourse to the courts for enforcement, the basic threshold of redress found in the *PIPED Act* is met. While this is a handy reduction to use when discussing the civil traditions of Quebec, it seems a rather low standard of similarity for the rest of Canada, and one that is arguably met in large part by the tradition of judicial review.

Reasonable Person Test

Under the *PIPED Act*, “an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.”⁴ This section is intended to place some level of justification on an organization for collecting personal information. The Commissioner notes that the Quebec legislation does not have a reasonable person test, but does provide that an organization may only establish a file on another person for a *serious and legitimate reason* and that the information collected must be *necessary* for the defined object of the file.⁵

To justify his determination of similarity, the Commissioner ties these sections with the reverse onus when dealing with objections to providing personal information. According to the Quebec law, an organization cannot refuse a good or service, or a re-

quest relating to employment, because an applicant refuses to provide personal information, unless the information is necessary for the performance of a contract or the collection is authorized by law.⁶ The organization must prove that the information is necessary for a serious and legitimate purpose to justify a refusal. The Commissioner considers the intent and effect of ‘serious and legitimate’ and the ‘necessary’ standard, combined with the burden on the organization to justify itself, to be similar to the reasonable person test found in the *PIPED Act*.

But is it similar? The federal standard asks what a reasonable person might anticipate; in contrast, the Quebec analysis shifts to what the organization can define as being necessary for a serious and legitimate purpose. A reasonable person test is obviously far more effective in securing the public interest because its terms of reference are based on the perceptions of people, rather than the justifications of organizations. The Privacy Commissioner, while applauding Quebec for putting the burden of proof on organizations to justify themselves in the face of complaints or requests for correction, nonetheless allows those organizations the advantage of dodging a reasonable purpose test in favour of what they can argue as serious and legitimate.

Consent

The *PIPED Act* requires an organization (subject to limited exceptions) to obtain the informed consent of an individual in order to collect, use, or disclose personal information.

Although parallel provisions deal with use and disclosure, the Quebec *Act* does not oblige an organization to obtain consent for collection. Quebec requires personal information to come from the individual concerned, unless that person consents to a third-party providing the information.⁷ Any consent must be “manifest, free and enlightened, and must be given for specific purposes.”⁸ Taking these two sections together, the Commissioner determines that this effectively provides for consent in all situations. If a third-party is passing information, consent from the relevant person is required; if the person is providing their own information, then consent to the collection is *implied*.

This is lower than the federal standard. Although collected information cannot be *used* or *communicated* without obtaining the required level of ‘manifest, free, and enlightened’ consent, the information could nonetheless be *gathered* without it. This is a notable gap. While the Commissioner welcomes proposed amendments that would include consent for the collection of information,⁹ he nonetheless finds the existing consent provisions substantially similar.

Both the federal and Quebec law allow for disclosure without consent in certain circumstances. A significant exception to this — and a win for the province’s direct marketing industry — is the exception of nominative lists. In Quebec, marketing lists containing names, addresses, and telephone numbers can be disclosed without consent for “commercial or philanthropic prospection,” as long as there is a chance for individuals to opt-out and the list does not “infringe upon the privacy of the persons concerned.” The latter point seems to mean that the transfer cannot reveal some personal aspect of the individual beyond the bare data in the nominative list (for example, the bare data could reveal a medical condition). The Commissioner, latching on to the protective provisions surrounding the release of nominative lists, sees the overall consent requirements as “roughly similar” to the *PIPED Act*.

Accountability?

In his Report, the Privacy Commissioner notes that the accountability and openness principles are not readily apparent in the Quebec legislation. Accountability and openness are two related principles in dealing with privacy matters: the former deals with how an organization is responsible for personal information, and the latter, for making that responsibility a public one.

The *PIPED Act* states that an organization shall designate an individual to be accountable for the personal information in its possession.¹⁰ Moreover, it explicitly requires that organizations implement policies and practices relating to all aspects of dealing in personal information — along with the training necessary for their effective application.¹¹ Furthermore, an organization must be able to explain its practices to the public in an understandable fashion.

This principle puts added responsibilities on the holder of personal information to keep internal mechanisms well defined, and thus accountable. Ideally, a clear privacy policy logically leads to the development of sound information management practices, clearer security procedures, and possibly cost-savings in the reduction and management of unnecessary information. Rather than limit accountability to a small number, the purpose of accountability is to make “an organization responsible and accountable as a whole.”¹²

Quebec has no such requirement. Organizations need only fulfill requirements in practice, and need not articulate them in any coherent policy. In addition, the Quebec legislation does not require the designation of an individual within an organization to be accountable for privacy matters — there is no impetus at the individual level for securing privacy protection. The Privacy Commissioner is content to allow the specific accountability principles enunciated in the *PIPED Act* to lapse.

Openness?

The accountability and openness principles are about transparency; together, they reflect the need for visible procedures and policies as a critical element to securing privacy.¹³ The *PIPED Act* obliges organizations to be open about how they deal with all personal information. The federal requirement goes further than other comparable principles expressed in Europe and in the OECD Guidelines.¹⁴ Organizations need to be able to clearly explain to any interested parties how and why they deal with personal information in a certain way. This is meant to compliment the individual access principle and its provision of a more specific right to personal data.

There is no parallel requirement that all Quebec organizations abide by a general openness principle. Quebec organizations are obliged to be transparent on a case-by-case basis — only individuals who are seeking information about their personal file have a right to a clear view of how their information is treated.

The Commissioner notes that individuals are notified during the information collection process of the purposes, use, location, and categories of person within

the organization who will have access to the information, and of access and correction rights. Perhaps his thinking was that this describes what would otherwise exist in an organization's internal privacy policy? Nonetheless, the Commissioner treats this as indirectly addressing the openness principle, even though it does not attain the breadth of the federal legislation in securing transparency to the organization's entire information management process.

Openness and accountability principles do find limited expression in the provisions dealing with 'personal information agents' — a narrow class of information dealers made up of credit reporting agencies. Personal information agents must draft and comply with rules of conduct, and make their activities known by publishing notices in regions where they do business.¹⁵ By speaking to both openness and accountability, this sector-specific requirement is the only component of the Quebec law that incorporates the ten principles found in the *PIPED Act*. An argument could be made that the Quebec *Act* is substantially similar solely as it relates to credit agencies.

While it might be suggested that a requirement of general openness is negligible, there are broader concerns at stake. Within an organization, employees who are unfamiliar with organizational practices and policies are less likely to be adhering to the commitments made. By acceding to the neglect of openness and accountability requirements, the Commissioner is tolerating a gap in the privacy laws of Quebec. Substantially similar means 'at least as good', and the terms of reference are the ten principles in Schedule 1. More than just a local tailoring of standards, the Quebec *Act* excludes a requirement for clear and open internal policies, and the corresponding accountability that follows.

Conclusion?

The federal Privacy Commissioner has determined that Quebec's *Act*, regardless of its seven-year seniority, is substantially similar to the *PIPED Act*. While the Commissioner does not have the last word on the subject, his comments give a glimpse as to what the nebulous phrase "substantially similar" might mean — assuming that it holds some weight as a precedent for the sort of standards that other provinces will face. Taking several points of discussion from his

report, it would seem that provinces have much latitude in crafting their own privacy regime: the mechanisms of redress need only be basic; a reasonable person test is just as good as a serious and legitimate purpose test; consent for the collection of information from its primary source is unnecessary; openness and internal accountability need only exist with respect to an individual and their own file, while the general openness principle is entirely optional. By accounting for Quebec's differences in legal tradition, and desiring to find common ground with Quebec's well-established privacy regime, the Privacy Commissioner has in some ways clarified, and in some ways diluted, the original language of the *PIPED Act*.

* Jeffrey Kaufman, Partner, Fasken Martineau DuMoulin LLP, Toronto, jkaufman@tor.fasken.com. Daniel Fabiano, Student, Fasken Martineau DuMoulin LLP, Toronto, dfabiano@tor.fasken.com.

¹ S.C. 2000, c.5.

² R.S.Q., c. P-39.1.

³ Privacy Commissioner of Canada, *Report to Parliament Concerning Substantially Similar Provincial Legislation* (Ottawa: Minister of Public Works and Government Services Canada, 2002) at 2.

⁴ s. 5(3).

⁵ s. 4, 5.

⁶ s. 9.

⁷ s. 6.

⁸ s. 14.

⁹ Bill 122, *An Act to amend the Act respecting Access to documents held by public bodies and the Protection of personal information, the Act respecting the protection of personal information in the private sector, the Professional Code and other legislative provisions* (s.69). The bill had second reading (adoption in principle) on June 13, 2000.

¹⁰ s. 4.1.

¹¹ s.4.1.4.

¹² December 4, 2001 finding of the Privacy Commissioner: where a man objected on principle to bank's identification program (online: http://www.privcom.gc.ca/cf-dc/cf-dc_011204_e.asp).

¹³ 4.8.1.

¹⁴ OECD Guidelines merely state: "There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."

¹⁵ s. 78, 79.

Non-Statutory Restrictions on the Use of Personal Information

Mark Hayes and Troy Ungerman*

The recent flurry of interest in privacy legislation triggered by the passing of the federal *Personal Information Protection and Electronic Documents Act*¹ (“PIPEDA”) has, to some extent, overshadowed the fact that protection of the privacy of personal information already exists in many forms.² While only a couple of years ago it would have been possible to say with reasonable certainty that no common law tort of invasion of privacy existed in Canada, courts in Ontario and other provinces are now signalling that a common law right to privacy may in fact exist and be enforced by the courts. As a result, while counsel must advise their clients carefully about how to comply with the various applicable statutory privacy restrictions, they must also be aware that uses of personal information which comply with these statutory rules should not automatically be considered to be legal or devoid of liability risk.

An independent common law tort of “invasion of privacy” has historically not been recognized in Canada. Rather, to the extent that privacy interests have been protected, the protection has been obtained through claims in trespass (to land, chattels and the physical person), nuisance (indirect invasion of an occupational interest in land which unreasonably interferes with one’s enjoyment of it), defamation and injurious falsehood and deceit (false statements calculated to cause pecuniary damage). Other recognized causes of action that might indirectly be brought to protect privacy interests include wilful infliction of nervous suffering, passing off, appropriation of personality and breach of confidence.³

Ontario courts appear, however, to have begun recognizing invasion of privacy as a cause of action that can stand on its own. Damages have been awarded for invasions of privacy, and the courts have, on several occasions, refused to strike out pleadings that included claims for invasion of privacy. In addition, the development of other legal doctrines designed to protect confidential information in the commercial context may well be employed to prevent the use and disclosure of personal information.

The test, which seems to be applied in claims relating to improper use of private and confidential information, is “whether the particular invasion of privacy is necessary to the proper administration of justice and, if so, whether some terms are appropriate to limit that invasion.”⁴ There is disagreement as to whether this creates an independent “right of privacy” or a separate tort of “invasion of privacy”:

“Despite some encouraging suggestions from a few courts, it would be fair to say that the Canadian tort law does not yet recognize a tort action for invasion of privacy *per se*. Rather “privacy” rights have been protected under the umbrella of other traditional tort actions, and by legislative interventions... [i]s a separate tort of “invasion of privacy” necessary? It is arguable that it is not. The concept of privacy is too ambiguous and broad to be able to be covered adequately in one cause of action. It is desirable to have the different aspects of privacy protection dealt with in separate torts, which more clearly can focus on the interests at hand. Gaps in the law which cannot be filled by extending traditional principles can be dealt with as they arise, either through the expansion of the common law or by legislative intervention.”⁵

U.K. courts have recently considered the common law right of privacy. *A v. B*⁶ involved an application by A, a “married professional footballer”, for an injunction prohibiting a London tabloid newspaper from publishing articles (said by the court to be “intended for the prurient”) about two women, C and D, with whom A had had relationships. In the course of its analysis, the court considered “whether [at common law] sexual matters occurring between two persons are subject to a duty of confidence in the absence of any express agreements between them to keep such matters confidential” and decided:

“I do not think that these questions can be given an absolute answer, nor should they be. Each case depends on its circumstances... What we have here is communication to a newspaper not just

of the fact of the relationships but of the details of the sexual conduct that occurred. The newspaper has no interest in simply publishing the facts of the relationship alone; it intends to publish the whole: to interest its readers it needs the detail. The answer in the present case is therefore straightforward. It was a breach of confidence for C and D to provide the information which they have to the newspaper or to anyone else with a view to its publication in the media.”⁷

The court in *A v. B* declined to deal with the wider question of whether there was an independent cause of action for breach of privacy beyond the law of confidentiality.

The U.K. Court of Appeal recently examined the existence of a common law right to privacy in *Douglas v. Hello! Ltd.* (“*Douglas*”)⁸The actors Michael Douglas and Catherine Zeta-Jones planned a sumptuous wedding and, for a substantial sum, granted an “exclusive” on photographs of the event to a London tabloid newspaper. Douglas and Zeta-Jones took extraordinary steps to ensure that no uninvited media were present. In addition to searching all guests and staff before entry for cameras or tape recorders, Douglas and Zeta-Jones had each guest and staff member sign an agreement stating that, in exchange for entry to the wedding location, they would not record the proceedings or take any photos. When the inevitable occurred and a competing unauthorized newspaper planned to publish photos of their wedding, Douglas and Zeta-Jones sought an injunction relying on both the contracts the guests and staff had signed and on alleged breaches of several common law obligations, including a right of privacy.

The claim by Douglas and Zeta-Jones had some serious flaws. Douglas and Zeta-Jones could not prove that whoever had taken the photographs had in fact executed the confidentiality agreement, and as a result they had to rely on common law rights in order to obtain an injunction. Nor could Douglas and Zeta-Jones claim that they wanted the photographs to be kept private (as they were to be published by another newspaper); rather, it was clear that what they wanted was to be able to control the use that was to be made of any photographs in order to maximize the financial return they could obtain for selling an “exclusive”.

The three members of the Court of Appeal reached the same conclusion (that the injunction could not be granted since the balance of convenience fell in favour of allowing the competing newspaper to publish the unauthorized photographs since damages would adequately compensate Douglas and Zeta-Jones and the authorized newspaper for any losses suffered), but each judge arrived at that result by a different path. Brooke L.J. recognized that the law of breach of confidence can apply “if, on a private occasion the prospective claimants make it clear, expressly or impliedly, that no photographic images are to be taken of them, then all of those that are present will be bound by obligations of confidence created by their knowledge (or imputed knowledge) of this restriction”,⁹ and he believed that the law of breach of confidence would cover the situation without resort to a tort of breach of privacy. Keene L.J. agreed that there was a breach of confidence, but did not deal explicitly with a more general right to privacy except to say that *Kaye v. Robinson*¹⁰ (in which the U.K. Court of Appeal had stated that English law did not recognize a common law right of privacy) would likely not be followed in the future. Sedley L.J. went further, however, and conclusively supported a free-standing common law right of privacy:

“[W]e have reached a point at which it can be said with confidence that the law recognises and will appropriately protect a right of personal privacy. . . . What a concept of privacy does, however, is accord recognition to the fact that the law has to protect not only those people whose trust has been abused but those who simply find themselves subjected to an unwanted intrusion into their personal lives. The law no longer needs to construct an artificial relationship between intruder and victim: it can recognise privacy itself as a legal principle drawn from the fundamental value of personal autonomy.”¹¹

Members of the High Court of Australia, in a case involving an injunction to restrain broadcast of a video taken surreptitiously inside a abattoir,¹² recently mused, without deciding, about the possibility that a separate tort of breach of privacy might be found to exist. After referring to the decision in *Douglas*, the High Court noted that both New Zealand¹³ and India¹⁴ had recognized a common privacy right, and one of the justices quoted Professor Linden to the effect that Canada was in the process of doing the same.¹⁵

Canadian courts have not yet elaborated standards for establishing a cause of action for invasion of privacy; rather, “whether or not an invasion of privacy results in an actionable and compensable tort depends on the circumstances of any particular case and the conflicting rights involved.”¹⁶ In *Lipiec v. Borsa*,¹⁷ the court found that the defendant’s installation of a surveillance camera focussed on his neighbour’s backyard was an intentional invasion of privacy. In *Roth v. Roth*,¹⁸ the court recognized a common law right of privacy, and found that the defendants’ verbal harassment, blocking of an access road to the plaintiffs’ property that went across their land, and the removal of previously shared property from the plaintiffs’ land (which resulted in the shutting off of electricity without reasonable notice) constituted an invasion of privacy. In *Saccone v. Orr*,¹⁹ the court found an invasion of privacy where the defendant recorded and played back a private telephone conversation.

Although none of the reported cases have to date involved the use of personal information that had been collected for business purposes,²⁰ one type of business-related activity that has been found to constitute an invasion of privacy is overzealous attempts to collect on debts. In *Palad v. Pantaleon*,²¹ the plaintiff sought repayment of a \$10,000 loan. When the loan was not repaid, the plaintiff began telephoning the defendant at her home and at her place of employment, and eventually showed up at the defendant’s place of employment and demanded repayment of the loan in front of her co-workers. Other cases have similarly found an invasion of privacy for overzealous activities associated with debt collection.²²

Based on the developing Canadian case law and the support that the concept of a tort of breach of privacy is receiving from the higher courts in the U.K., it can reasonably be expected that there will be increasing recognition by Canadian courts of an independent privacy right. In addition, even if there is no common law right of privacy, Canadian courts will not hesitate to protect the privacy of personal information under some recognized tort.²³ Briefly discussed below are three developing areas of law, which might, in certain cases, serve as a basis for a claim against organizations, which deal with personal information.

(a) Breach of Confidence

As can be seen from the U.K. decisions in *A v. B* and *Douglas*, even absent a tort of invasion of privacy, courts will often enforce privacy rights by employing the tort of breach of confidence. According to Canadian jurisprudence, Canadian courts will enforce a claim for breach of confidence where three conditions are met:

- (i) the information must have the “necessary quality of confidence about it;”
- (ii) the information must have been imparted in confidence; and
- (iii) there must be unauthorized use to the detriment of the party communicating the information.

The Supreme Court of Canada in *Lac Minerals v. International Corona Resources*²⁴ held that, where a party receives private information in confidence, there is an expectation that it will not misuse that information for its own benefit,²⁵ and where information of a commercial value is given on a business-like basis, the recipient is regarded as carrying a heavy burden if it seeks to resist a claim that it was bound by an obligation of confidence. The U.K. Court of Appeal stated in *Douglas* that “the tort of breach of confidence contains all that is necessary for the fair protection of personal privacy.”²⁶

It is readily apparent that many business relationships, which involve exchanges of personal information, can be seen as creating the necessary relationship of confidence to create an obligation of confidentiality, especially where sensitive personal information is provided by one or both parties as part of the relationship. Examples of such relationships include those between insurer and insured, banker (or other financial advisor) and customer, health care practitioner and patient, consultant and client, and, of course, lawyer and client. In many circumstances, the professional obligations created by the relationship will circumscribe the use of personal information by one or both parties, but there may well be additional common law duties, which will apply in addition to, or in the absence of, such obligations. The difficult question, of course, is determining the extent of the privacy duty in the particular circumstances of each individual relationship.

(b) Fiduciary Duty to Keep Information Confidential?

The Supreme Court of Canada in *Frame v. Smith*²⁷ stated that there are three characteristics to be considered in determining whether a fiduciary duty exists:

- (i) the fiduciary has scope for the exercise of some discretion or power;
- (ii) the fiduciary can unilaterally exercise that power or discretion to affect the beneficiary's interests; and
- (iii) the beneficiary is vulnerable to or at the mercy of the fiduciary exercising the discretion of power.

However, a fiduciary relationship may be found even though some of these characteristics are not present; conversely, the presence of such characteristics does not invariably identify the presence of a fiduciary relationship.

For example, in *Haskett*,²⁸ the court considered, *inter alia*, whether a credit-reporting agency owed a fiduciary duty to its consumers, and whether the credit-reporting agency committed the tort of invasion of privacy. In determining that the credit reporting agency did not owe a fiduciary duty to its consumers, the court reasoned that the credit-reporting agency acted in its own self-interest in selling its services, notwithstanding the fact that the manner of providing such services was constrained by statute. The court held that the credit-reporting agency did not relinquish its self-interest and did not act on behalf of the consumer for the consumer's benefit. The court further held that, although the credit reporting agency may owe a *prima facie* duty of care to the consumer, with the standards of the *Consumer Reporting Act*²⁹ informing that duty of care, such duty is not a fiduciary duty.

In light of the decision in *Haskett*, it is unlikely that an enterprise carrying on business in its ordinary course would have fiduciary duties imposed on it beyond any relevant statutory restrictions.

(c) Industry Policies and Negligence

In *Canada v. Saskatchewan Wheat Pool*,³⁰ the Supreme Court of Canada held that proof of statutory breach may be used as evidence of negligence and that the statutory formulation of the duty may afford a specific, and useful, standard of reasonable conduct.³¹ The acceptance of statutory duties as the standard of reasonable conduct can be further extended to include recognized industry policies, practices, or standards as setting the standard of reasonable conduct, and the breach of a generally accepted industry standard may constitute evidence of negligence. For instance, the recent decision in *Zraik v. Levesque Securities Inc.*³² confirmed that failing to comply with certain professional duties and internally created guidelines could be used to establish negligence. As a result, industry standards, such as model privacy policies or codes, may create a specific and useful standard of reasonable conduct with respect to the collection of personal information, and a breach of such policies may constitute evidence of negligence.

(d) Conclusion

The development of a common law right of privacy continues in Canada, albeit at a slow rate compared to the relatively rapid pace of legislative activity. Nevertheless, it is impossible to ignore the existence of a common law right that will likely continue to co-exist with and supplement the statutory protections for personal information privacy. Prudent counsel (and their clients) should consider whether dealings with personal information that comply with all relevant statutory restrictions may nevertheless be considered to be breaches of a developing common law right, especially since damages for such breaches will be at large and may greatly exceed the remedies prescribed under applicable statutes, especially if such damages are claimed in a class action.

** Mark Hayes and Troy Ungerman, Ogilvy Renault, Toronto. Any opinions expressed in this article are solely those of the authors and not Ogilvy Renault or any of its clients. This article contains only a general commentary on the law; is not legal advice and should not be relied upon as such. Please consult qualified counsel if you require advice about any of the topics discussed in this paper. Copyright 2002, Mark Hayes and Troy Ungerman.*

¹ S.C. 2000, c.5.

² Note that this article is only referring to the obligations of private sector entities in respect of personal information. For an interesting discussion of the

privacy obligations of the public sector under the *Charter of Rights and Freedoms* and other legislation, see the opinion of Justice La Forest commissioned by the federal Privacy Commissioner at <www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp>.

³ Burns, "The Law and Privacy: The Canadian Experience" 54 C.B.R. 1 at 12-24; Rainaldi, *Remedies in Tort* (Toronto: Carswell, 2000) at 24-12.1 to 24-19; McIsaac, Shields & Klein, *The Law of Privacy in Canada* (Toronto: Carswell, 1987) at 2-53 to 2-58.1.

⁴ *M. (A.) v. Ryan* (1994), 98 B.C.L.R. (2d) 1 at 19, cited in *British Columbia (Assessor of Area No. 09 - Vancouver) v. Lord Realty Holdings Ltd.*, [1996] B.C.J. No. 2092 (B.C.C.A.).

⁵ Klar, *Tort Law* (Toronto: Carswell, 1991) at 56, cited in *Haskett v. Trans Union of Canada Inc.*, [2001] O.J. No. 4949 (S.C.J.) ("*Haskett*"). However, the Court in *Haskett* acknowledged that, more recently, there has been some recognition of invasion of privacy as an embryonic tort where there is harassing behaviour or an intentional invasion of privacy: *Tran v. Financial Debt Recovery Ltd.* (2000), 193 D.L.R. (4th) 168 and *Lipiec v. Borsa* (1996), 31 C.C.L.T. (2d) 294 (Ont. Gen. Div.).

⁶ [2001] 1 W.L.R. 2341 (Q.B.).

⁷ *Ibid.*, at 2354.

⁸ [2001] Q.B. 967 (C.A.).

⁹ *Ibid.*, at 988.

¹⁰ [1991] F.S.R. 62 (C.A.).

¹¹ *Supra*, note 9, at 997 and 1001.

¹² *Australian Broadcasting Corporation v. Lenah Game Meats Pty. Ltd.*, [2001] H.C.A. 63.

¹³ *P. v. D.*, [2001] 2 N.Z.L.R. 591; Tobin, "Invasion of Privacy", [2000] New Zealand Law Journal 216.

¹⁴ *Govind v. State of Madhya Pradesh* (1975) 62 A.I.R. (SC) 1378.

¹⁵ Linden, *Canadian Tort Law* (6th ed., 1997) at 56.

¹⁶ McIsaac *et al.*, *supra*, note 4, at 2-55 (citing *Roth v. Roth* (1991), 9 C.C.L.T. (2d) 141 (Ont. Gen. Div.)).

¹⁷ *Supra*, note 6.

¹⁸ *Supra*, note 17.

¹⁹ (1981), 34 O.R. (2d) 317 (Co. Ct.).

²⁰ Rainaldi, *supra*, note 4, at 24-12.2 to 24-12.4.

²¹ [1989] O.J. No. 985 (Dist. Ct.).

²² *Supra*, note 6.

²³ *Dyne Holdings v. Royal Insurance of Canada* (1996), 34 C.C.L.I. (2d) 180 (P.E.I.S.C.).

²⁴ [1989] 2 S.C.R. 575.

²⁵ See also *Cadbury Schweppes Inc. v. FBI Foods Ltd.*, [1999] 1 S.C.R. 142.

²⁶ *Supra*, note 9, at 998-999.

²⁷ [1987] 2 S.C.R. 99 at 136.

²⁸ *Supra*, note 6.

²⁹ R.S.O. 1990, c. C.33.

³⁰ [1983] 1 S.C.R. 205.

³¹ *Ibid.*, at 244.

³² [1999] O.J. No. 2263 (S.C.J.) as varied by [2001] O.J. No. 5083 (C.A.).

The articles, which appear in this publication, represent the opinions of the authors. They do not represent or embody any official position of, or statement by the OBA except where this may be specifically indicated; nor do they attempt to set forth definitive practice standards or to provide legal advice. Precedents and other material contained herein are intended to be used thoughtfully; as nothing in the work relieves readers of their responsibility to consider it in the light of their own professional skill and judgment.

For Sale

Audio Tapes

And then There were Two: Issues for Business under the new *Draft Ontario Privacy of Personal Information Act*
April 29, 2002

Speakers: John Beardwood, Brian Keith and Rick Shields

Audio tape code S-01-764

Price: \$20 + GST + PST

Chief Privacy Officer — The New Executive Position

March 5, 2002

Speakers: Anita Fineberg, Robin Gould-Soil, Stephanie Perrin and Miyo Yamashita

Audio tape code S-01-763

Price: \$20 + GST + PST

A Private Sector Privacy Bill for Ontario: A Wish List

December 11, 2001

Speaker: Ann Cavoukian

Audio tape code S-01-762

Price: \$20 + GST + PST

Threshold Issues in Privacy — The Crucial Questions

November 8, 2001

Speakers: Barry Sookman, Jeff Kaufman, David Young and Priscilla Platt

Audio tape codes S-01-760 & 761

Price: \$35 + GST + PST

Publications

Current Issues in Employment Law

This publication includes the following invaluable information: important issues in the new Employment Standards Act; the restructuring of the workforce from an “in-house” perspective; workplace privacy issues; avoiding violence in the workplace; mandatory retirement; and electronic evidence in employment actions.

Price: \$75 + GST

Privacy Law Fundamentals — 2002 Inst.

There never has been a better time to become familiar with privacy law. This material will tell you what these laws are all about, how personal information may be collected, used and disclosed, how these laws apply generally as well as to specific sectors such as the health sector, and what the implications are for litigators, for counsel practicing employment law, for those involved in the sale of a business and in a myriad of other contexts. Find out how your clients can prepare and what you need to know to give the most up-to-date advice.

Price: \$60 + GST

To order, please complete the order form included in this mailing and return it to the Ontario Bar Association along with your payment. For further information, please contact the Publications Department or visit our website: www.oba.org

GST Registration #R100760495.

Section Executive 2002 - 2003

Chair: **Priscilla Platt**
Management Board Secretariat
(416) 326-1722
priscilla.platt@mbs.gov.on.ca

Vice-Chair: **Jeffrey A. Kaufman**
Fasken Martineau DuMoulin LLP
(416) 868-3417
jkaufman@tor.fasken.com

Secretary (Sections):
Mary C. O'Donoghue
Information & Privacy Commission/
Ontario (416) 326-3922
modonogh@ipc.on.ca

Newsletter Co-Editor: **Adam Kardash**
Heenan Blaikie LLP (416) 360-3559
akardash@heenan.ca

Newsletter Co-Editor: **Elena Szamosvari**
Financial Services Commission of Ontario
(416) 590-7149
eszamosv@fsc.gov.on.ca

Program Coordinator: **Larry P. Reimer**
Blaney McMurtry LLP (416) 593-3997
lreimer@blaney.com

Program Coordinator: **Brian D. Wylynko**
Federal Express Canada Inc.
(905) 212-5348
bdwylynko@fedex.com

AGR Liaison: **Roslyn A. Baichoo**
Lang Michener (416) 360-8600
rbaichoo@langmichener.ca

AGR Liaison: **Fazila Nurani**
PrivaTech Consulting (905) 886-0751
fnurani@privattech.ca

National Liaison: **John P. Beardwood**
Fasken Martineau DuMoulin LLP
(416) 868-3490
jbeardwood@tor.fasken.com

Regional Coordinator:
Barbara A. McIsaac
McCarthy Tétrault LLP (613) 238-2105
bmcisaac@mccarthy.ca

Member-At-Large: **Edith H. Cody-Rice**
Canadian Broadcasting Corporation
(613) 724-5353
codyrice@ottawa.cbc.ca

Member-At-Large: **Jennifer Dolman**
Osler, Hoskin & Harcourt LLP
(416) 862-5911
jdolman@osler.com

Member-At-Large: **Anita D. Fineberg**
IMS HEALTH, Canada (905) 816-5080
afineberg@ca.imshealth.com

Member-At-Large: **Mark S. Hayes**
Ogilvy Renault (416) 216-4094
mhayes@ogilvyrenault.com

Member-At-Large: **Lise S. Hendlisz**
Management Board Secretariat
(416) 327-6887
lise.hendlisz@mbs.gov.on.ca

Member-At-Large: **John R. Higgins**
Information & Privacy Commission/
Ontario (416) 326-3941
jhiggins@ipc.on.ca

Member-At-Large: **Rick Shields**
McCarthy Tétrault LLP (613) 238-2171
rshields@mccarthy.ca

Member-At-Large: **Juliet E. Slemming**
Teranet Inc. (416) 360-8863 x2702
juliet.slemming@teranet.ca

Member-At-Large: **Karen Spector**
kasprivacy@rogers.com

Member-At-Large: **John Z. Swaigen**
Information & Privacy Commission/
Ontario (416) 326-3920
jswaigen@ipc.on.ca

Editors:
Adam Kardash
Elena Szamosvari
Copy Editor:
Vickie Rose

Ontario Bar Association
Association du Barreau
de l'Ontario

300-20 rue Toronto St.
Toronto, Ontario
TDX Box 104
M5C 2B8

Phone | Tél.
1-800-668-8900
(416) 869-1047

Fax | Téléc.
(416) 869-1390

Internet
www.oba.org

A Branch of the Canadian
Bar Association

Une division de l'Association
du Barreau canadien