* Tim Dixon, Baker & McKenzie E-Strategy, Australasia 2000 conference, December 13 2000, tim.dixon@bakernet.com

1 Information presented at 21st International Conference on Privacy and Data Protection, Hong Kong, 13-15 September 1999

2 "Privacy on the Net: A Growing Threat", Business Week, 20 March 2000 (cover story)

3 OECD Guidelines covering the protection of privacy and transborder flows of personal data, Paris, 1980

4 *Privacy Committee Act 1975 (NSW)*

5 Westin, A. *Privacy and Freedom*, New York, 1967, p39, quoted in Goldman, J. "Privacy and individual empowerment in the interactive age", paper presented at the *Visions for Privacy in the 21st Century* conference, Victoria, British Columbia, May 9-11 1996, p26

6 Trubow, G. *Protocols for the secondary use of personal information*, unpublished paper, John Marshall Law School Centre for Informatics Law, February 22 1993, p4

7 OECD Guidelines covering the protection of privacy and transborder flows of personal data, Paris, 1980

Canada's New Privacy Law: A Powerful Response to an Important Issue

Peter Mantas, Heenan Blaikie, Canada

Peter Mantas is a technology lawyer in the Ottawa office of the law firm of Heenan Blaikie, one of Canada's largest law firms. He is a guest lecturer at the University of Ottawa Law School and visiting professor at the Universidad del Mayab, Mexico. He is a frequent speaker and writer on numerous technology law issues including the new privacy law in Canada, and advises clients on intellectual property, corporate and litigation matters. He can be reached at pmantas@heenan.ca.

On January 1, 2001, a new law regarding the protection of personal information came into force in Canada. The *Personal Information Protection and Electronic Documents Act*1 (the "Act") was passed by the Canadian federal government to address a wide range of issues affecting the privacy of Canadians. The Act was seen as a necessary response to the growing ability of organizations, particularly through the Internet, to collect and manipulate personal data.

In addition, the Canadian government believed that by passing such a law, electronic commerce in Canada would be enhanced, which was an important goal of the Liberal government and Prime Minister Jean Chretien. Studies presented to the government suggested that there was a perception by the general public that privacy was not respected on the Internet, and that data submitted to websites was routinely exploited for uses unknown and unwanted by web surfers. This lead the federal government to conclude that a privacy law would provide users of the Internet in Canada with the confidence to do more, rather than less, business online.

The government was also persuaded to pass the Act for several other reasons. First, the European Union had recently passed a directive which restricted the flow of personal information collected in Europe to countries which did not have a privacy law. Canada saw this both as an obstacle to electronic commerce with Europe, and an opportunity to pick up business from the United States, which did not have acceptable privacy legislation, either in force or impending.

Second, Canadians were increasingly demanding a law to protect their privacy. With the power of the Internet, Canadians became more aware of the ability of organizations to collect, use and disclose information about their person. With this awareness came a growing sense of concern that their individuality was being compromised, that their security and affairs might be adversely affected, and that they would be subjected to annoying material from companies using their personal data for profit.

The Act passed by the Canadian government was broad, novel, and powerful in its enforcement capabilities. Consequently, the Act has been controversial, and it is likely to be the subject of litigation in the future. In particular, groups that have come to rely upon the free flow of personal information, such as the medical industry, are concerned that their interests will be seriously affected. However, the new law has been well received by many Canadian individuals who believe that privacy, from a human rights perspective, is an important right that ought to be protected.

The Act is divided into two parts. The first part deals with privacy and the second addresses electronic documents. Each part operates independently and this paper will discuss only part one, as this paper is intended to review Canada's new federal privacy law.2 The Act also incorporates, as a Schedule, the Canadian Standards Association Model Code for the Protection of Personal Information (the "Code"), a private sector initiative which predated the Act.3 Bringing the Code into the statute was an unusual technique which had the advantage of presenting the rules of the Act in plain language that was already known to the public and had been tried and tested. Unfortunately, simply appending a Schedule, drafted not as a federal statute but as a private sector

guide, and then giving it the force of law, opened the door to confusion and potential legal mischief. Furthermore, the Code was passed in 1996, which was in the early days of the Internet.

The purpose of the Act is well summarized in section 3, which states that:

"3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

The Act applies to every organization in respect of personal information that the organization collects, uses or discloses in the course of commercial activities. "Organization" is broadly defined to include an association, partnership, person or trade union. The Act does not apply to the Canadian government and its institutions, which are already subject to a privacy law, or to journalistic, artistic or literary purposes. In addition, and importantly, the Act does not apply to purely personal or domestic endeavours. In other words, people are free to collect, use or disclose personal information for their own non-commercial purposes.

The Act states that personal information obtained by an organization may be collected, used or disclosed only for purposes "that a reasonable person would consider are appropriate in the circumstances."[4] This general clause is over and above the specific provisions which are set out in the Act to deal with personal information. It allows the courts and the administrator of the Act, the Privacy Commissioner, extensive latitude in their enforcement. It also elevates the power of the individual because it is the reasonable "person" not the reasonable "organization", that serves as the benchmark as to what is and is not an acceptable purpose.

The Act sets out ten principles which every organization dealing with personal information in Canada must follow. The principles are listed in the Code. Essentially, these principles, in considerable detail, explain what is meant by privacy, and what is expected by the law.

The first principle states that an organization is responsible for personal information under its control and shall designate an individual who shall be accountable for the organization's compliance with the Act. The identity of the accountable individual must be available upon request. The organization is also responsible for information which is transferred to a third party for processing. In addition, it must implement policies and procedures to give effect to its responsibilities under the Act, and train staff to be able to follow the procedures.

Second, the purpose for which the organization collects personal information must be identified at or before it is collected. Information that is collected should not go beyond the identified purpose. Persons who collect the information should be able to explain why they are collecting it, and do so in a way which is reasonably simple to understand.

Third, the knowledge and consent of the individual is required for the collection, use or disclosure of personal information, except in certain circumstances such as medical, legal or national security reasons. The form of consent will vary depending on the circumstances of collection and the sensitivity of the information. Consent cannot be a condition before an organization will supply some good or service to an individual.

Fourth, the information which is collected shall be limited to the purpose identified by the organization. Collection shall not be indiscriminate and must be done in a fair and lawful manner. Individuals cannot be deceived regarding the purpose for which information is being collected.

Fifth, personal information shall not be used or disclosed for any purpose other than what was identified to the individual. Moreover, information shall be retained only as long as necessary for fulfilling the purpose. If a new purpose is required, consent must be obtained and the new purpose documented. Minimum and maximum retention periods for data are recommended. When the information is no longer required, it is expected to be destroyed, deleted or made anonymous.

Sixth, data must be accurate, complete and up-to-date so as to fulfil its identified purpose. Personal information is not to be routinely updated.

Seventh, personal information must be protected by security safeguards depending on the sensitivity of the information. Protection of data refers to issues of loss, theft, unauthorized access, disclosure, copying, use or modification. Physical, organizational and technological measures must all be used to satisfy the security requirements of this principle. In addition, care must be used in the disposal or destruction of information to ensure that its security is not jeopardized.

Eighth, individuals must be given information about the organization's policies and practices relating to its handling of personal information. This information must be reasonably available and generally understandable. An organization is specifically required to provide upon demand the name and address of the person accountable for personal information, how to access personal data, a description of the type of information being held about the individual, including how it is used, brochures explaining the company's policies, and what is released to related organizations like subsidiaries.

Ninth, an individual must be advised of the existence of any information about him or her, and the individual must be able to challenge the accuracy of the information. Upon demand, the information must be amended if incorrect. A response to such requests shall be at a reasonable cost and within 30 to 60 days. A list of to whom disclosure of personal information of the individual was made shall also be provided.

Tenth, an organization shall put procedures in place to handle

complaints or inquiries about their policies. Furthermore, the organization must investigate all complaints.

In addition to the above, the Act states that persons with sensory disabilities have a right to receive access to their information in an alternative format so that their disability may be accommodated.

Non-compliance with the principles described above can result in numerous serious consequences. These range from an investigation or audit by the Privacy Commissioner, to damages in a civil court to fines of up to $100,000 in a criminal court. Interestingly, the Act allows individuals to sue in court for damages for the previously unrecognized tort of humiliation. Ironically, it is expected that public humiliation by the Privacy Commissioner of a non-compliant company will be one of the most powerful methods of ensuring general compliance with the Act.

In addition, the Privacy Commissioner, in carrying out his or her duties, has extensive powers of investigation including the power to summon witnesses, and to enter into any premises (excluding a dwelling-house). While such powers for an administrative agency are not unheard of under Canadian law, entry upon premises without a judge ordered warrant where there are potential penal sanctions in the end are unusual. Time will tell if the Commissioner will ever use this power, and if it is used, whether it could withstand a constitutional challenge under the due process provisions of the Canadian *Charter of Rights and Freedoms*.

The Act also provides protection to "whistle-blowers" who alert the Privacy Commissioner to a violation of the Act. Again, it is uncertain as to how far the Privacy Commissioner will go to enforce the Act in various circumstances, and what will be his or her preferred enforcement mechanisms. At the moment, the Privacy Commissioner has stated in its publications and numerous conferences that it will prefer moral persuasion, as opposed to actual force, in ensuring that the objects of the Act are carried out.

In response to strong opposition from the Canadian health sector, the Act will not come into force with respect to personal health information until January 1, 2002. In addition, the Act does not apply to matters of a purely provincial nature until January 1, 2004. This latter provision was enacted so as to push the provinces to enact their own legislation regarding privacy. Whether or not the Canadian Constitution allows the federal government to enact privacy legislation where some provinces decide to do nothing is unclear, and could be another source of constitutional litigation in the future. The Province of Quebec already has a privacy law and has been exempted from the Act by the federal government.

In its quest to protect the individual's right in personal information, the Canadian government itself may have crossed the line. Indeed, the Act's powerful enforcement mechanisms may, ironically, jeopardize an organization's expectation of privacy from government intrusion.

Clearly, the Act has come down on the side of privacy advocates. The new law is broad and powerful. However, the full impact of the law will remain to be seen. Much discretion is in the hands of the Privacy Commissioner, who is the custodian of the Act, but has been for only a very short period of time. Furthermore, Canadians will have considerable discretion in how often, and how, the Act is used.

In 1890, the famous jurist Louis Brandeis, along with Samuel Warren, wrote that the definition of privacy was the "right to be left alone."[5] Now that Canadians have a law that grants them the ability to be left alone, the question is whether they really want to be left alone, or if they will sacrifice privacy for the benefits the disclosure of their personal information may give to them.

---

1 S.C. 2000 (48-49 Eliz. II), Ch. 5 (Royal assent received April 13, 2000).

2 There has been some debate as to why the subject of privacy was placed together with electronic documents in the Act. Arguably, the two issues deal with related issues in the field of electronic commerce. More probably, the answer lies in federal political reasons related to the most effective manner of passing a law which faced strong opposition from certain sectors in Canada such as health.

3 The Code, which was passed in 1996 by the Canadian Standards Association, was included in its entirety in the Act. Therefore, the Code has become federal law, except where the Act specifically modifies it.

4 Section 5(3).

5 Louis Brandeis, et al., The Right to Privacy, 4 Harv.L.Rev. 193-220 (1890).