Privacy in Canada: Some Comparisons

Tom Riley

Privacy has been defined in many ways. United States Justice Louis Brandeis said it was "the right to be let alone." Professor Alan Westin of Columbia University, acknowledged as the preeminent expert on privacy today, has defined it as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is to be communicated to others." In contemporary Canadian society privacy has become known in the narrower context of 'data protection' or the right to have one's own personal information protected and kept from the prying eyes of others.

Privacy has become an issue in the 1980s because of the microelectronics revolution and the capacity of computers to not only retrieve, process and disseminate personal information but the ability to share information around the world in microseconds. There are personal files kept on all of us at every level of government and with every institution with which we do business. Surveys show that potential violation of individual privacy is a concern in society. Experts, such as Dr. Arthur Cordell of the Science Council of Canada, gives some examples of potential problems in his 1985 book, *The Uneasy Eighties: The Transformation to an Information Society.* "Easy access to personal files by various organizations presents another threat to personal freedom. The Associated Credit Bureaus of Canada exchange credit information with 3,000 businesses in Montreal alone. Thus at least 3000 people in Montreal have at their command detailed information on the financial affairs of millions of other people."

He goes on to observe that "the concern is not so much about the computer itself as about the consequences of linking together databases to form networks. It is one thing for someone to enter an office and open a paper file to extract some information on someone. The linking up of electronic data files means that information on individuals can be extracted without the requestor having to be physically at the place where the information is stored.... The incorporation of large personal databases into communications networks presents a serious threat to conventional consideration of privacy."

He concludes that the "proper and sensitive treatment of privacy, or, more correctly, individual autonomy is becoming an important issue and is creating a very real sense of unease during the transition to an information society."

The importance of privacy protections has been stressed by another United States Justice, David L. Bazelon who observed that "Potentially at odds with the free flow of information is the right to privacy. While the right to be left alone, to control information about ourselves, serves many purposes in a society that respects individuality, privacy has an important political dimension. By allowing the citizen control over private information and communications, freedom from surveillance, and spheres of action free of societal interference, privacy fosters the growth of the autonomous, free-thinking individuals necessary for self-government."

The Canadian Parliament has partially addressed the privacy problem in society, first in 1977 through granting Canadian citizens the right of access and correction of their own personal files, with certain limited exceptions, under part 4 of the *Canadian Human Rights Act* and then with more extensive protections under the *Privacy Act*, passed in 1982 and operational as of July 1, 1983. The latter, which replaced Part 4 of the *Canadian Human Rights Act* grants far more privacy rights. In Canada only one of the provinces, Quebec, has granted privacy rights with the passage of their *Access to Documents Held by Public Bodies and Protection of Personal Information Act* in 1982.

The current *Privacy Act* allows the citizen the right of access and correction to one's own personal file, limits the

---

Tom Riley, head of Riley Information Services in Toronto, has testified before both parliamentary and Congressional Committees on the subject of privacy legislation.

types of personal information which might be shared with other government departments, sets out what are called 'fair information practices', i.e. rules as to how information should be kept to protect the individual, grants the right to lay a complaint to a person independent of government (the Federal Privacy Commissioner) in the event of violation of one of the principles of the Act and calls for the Privacy Commissioner to audit personal data banks kept by government to ensure the principles of the *Privacy Act* are being maintained.

The question now facing Parliament, as the result of the tabling in the House of Commons, on March 31, of the Report of the Standing Committee on Justice and the Solicitor-General on its three year review of the *Access to Information* and *Privacy Act*, is to what extent the *Privacy Act* should be extended to cover other areas of Canadian society, if at all?

Situation in Other Countries

The continuing debate in Canada and other Commonwealth countries, such as Australia, New Zealand and Great Britain, has been to what extent privacy laws should be extended to the private sector. Great Britain, a member of the Council of Europe, which has a convention for the Protection of Individuals with Regard to Automatic Processing of Data, decided in 1982 to proceed with legislation to cover automated data banks in both the public and private sectors. Prime Minister Thatcher opted not to cover manual files on the grounds that granting such a right would be far too cumbersome on both Government and the Private sector.

In New Zealand privacy rights were first extended in the mid-1970's to citizens who were registered in police computers. This was unique in the Commonwealth and existed until the passage of the *Official Information Act* in 1982. The Act which allows access to government records similar to *Canada's Access to Information Act* also grants limited rights of access to personal information kept in government files. However, the rights extended to individuals are not as extensive as those enshrined in Canada's *Privacy Act*. There are no ground rules on how the personal information should be kept nor are there any auditing requirements as in Canada.

Australia's *Freedom of Information Act*, also passed in 1982, is similar to New Zealand's in that it grants only access to personal information but no other privacy rights. These limited privacy rights were tacked on to both these bills because the privacy debate in these Commonwealth countries was becoming intensified in the early 1980's.

The Organization for Economic Co-operation and Development had adopted privacy guidelines entitled "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" in 1980 (Canada adhered in 1984 as did Australia). These guidelines, written by a Committee chaired by an Australian, the Hon. Justice Michael Kirby, then Chairman of the Law Reform Commission and now President of the Court of Appeal of the Supreme Court of New South Wales, were influential in sparking a debate in all the OECD and some Commonwealth countries.

Nine European countries currently have laws known as Data Protection Acts, which extend rights to individuals in the public and private sector. However, they cover mostly automated data banks (computers) and little attention is paid to manual files. Twelve more countries, including Japan, are currently developing legislation.

Passage of the OECD Guidelines was the single most important factor in limited privacy rights being adopted in Australia and New Zealand, a full *Data Protection Act* in Great Britain and Canada's *Privacy Act*. The latter is unique in the Commonwealth because of the extensive rights it guarantees and the fact it covers all government files, automated and manual.

The OECD principles set out the following ground rules for the keeping of personal information. They are a good summary of the principles incorporated in most full-blown privacy/data protection laws.

1. Informed consent of the individuals for the use of information about themselves, where appropriate;

2. The collection of only relevant, accurate and timely data, related to the purpose for which they are to be used;

3. Identification in advance of the purpose for data collection;

4. Restrictions on the reuse of data for new purposes without the consent of the individual or without legal authority;

5. Reasonable security safeguards;

6. Openness about practices with respect to the collection, storage or use of personal data;

7. A right of access for individuals to information about themselves; and

8. The accountability of the data controller for compliance with data protection measures.

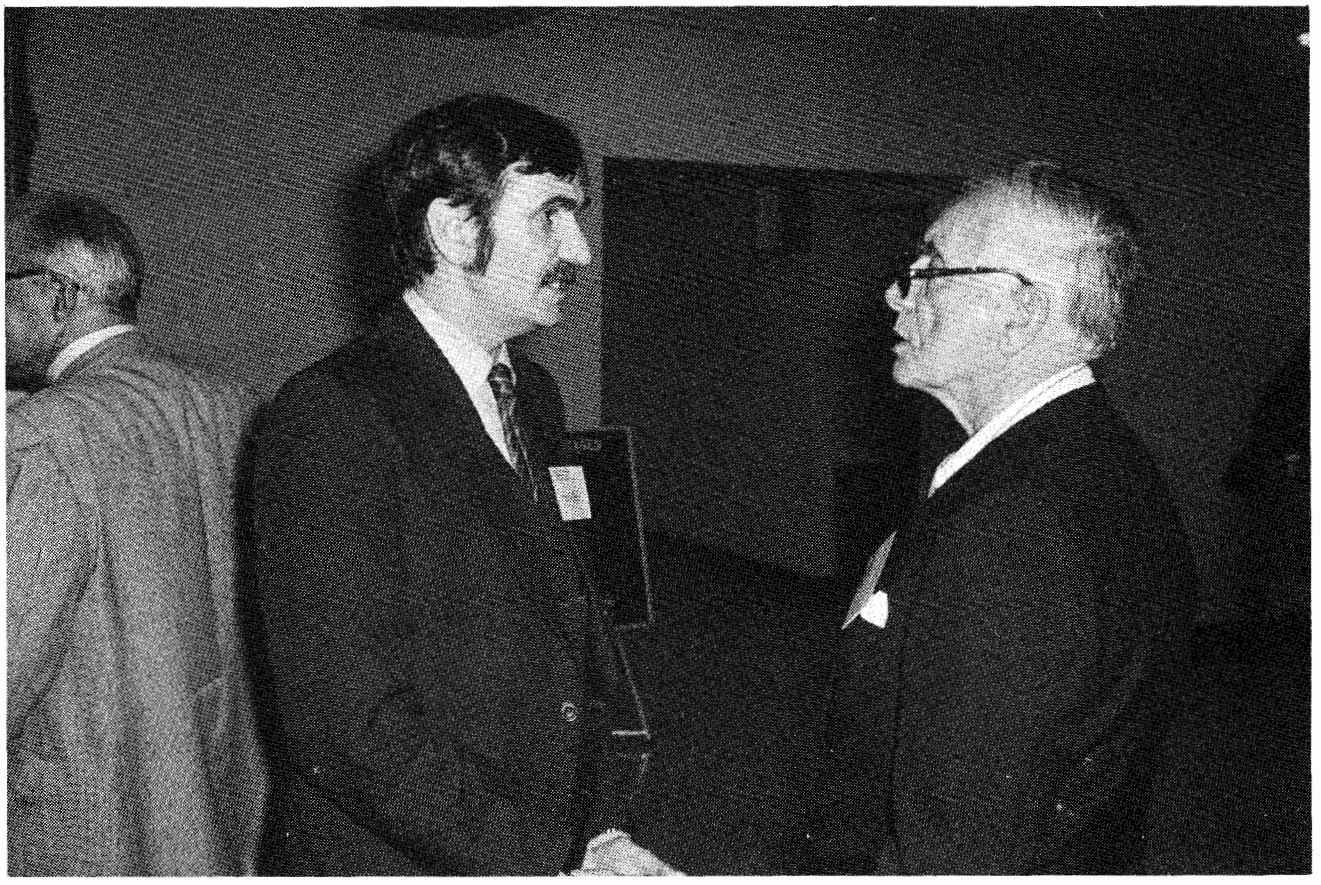
Canada, through adhering to the Guidelines, met her moral obligations through the existence of the *Privacy Act* and the sending of a letter, in November, 1986, from the Secretary of State for External Affairs, Joe Clark, to 130 multinationals urging them to develop privacy codes within their own companies and to officially adhere to the Guidelines. The Parliamentary Committee felt more should be done to encourage adoption of the Guidelines and the implementation of the Codes. In the United States 200 multinational corporations adhered to the Guidelines in 1981 with promises of action to develop full privacy codes. Such codes would incorporate the basic

privacy principles but would give no legal recourse to individuals in the event of abuse of their personal data by a company. No similar recourses have been recommended in the parliamentary committee report, a serious oversight to some privacy experts who feel that citizens need civil remedies in the event of privacy violations.

There appears to be little evidence that corporations are doing much in Canada to adhere to the Guidelines or develop privacy rights. A few companies and associations, such as the Bank of Montreal, IBM, American Express (Canada) Inc., Comcheq Services Ltd. of Winnipeg (a large payroll service with the names of 350,000 Canadians in their data bases) and the Canadian Life and Health Association, have developed privacy codes. The Royal Bank of Canada released draft privacy guidelines to the Justice Committee in May 1986, when appearing before them, but have yet to enact them. There are no other signs that other companies are going to comply or that the government will force some form of compliance. The parliamentary committee has made recommendations that, if adopted, could change this and force enactment of privacy guidelines in some sectors of Canadian society.

The privacy debate in Canada, Australia and New Zealand in the last few years has been about how far these rights should be extended to the private sector. Many Canadian corporations have resisted the development of regulations claiming they do not want a cumbersome bureaucracy overseeing their data banks. Others claim that to extend the *Privacy Act* to the private sector would be to create an Information Czar, the Privacy Commissioner, who would have far too much power over the private sector. Professor David Flaherty, of the University of Western Ontario, an advisor to the parliamentary committee which produced the Report, has said that action is needed as the private sector have known about these problems and have not acted.

In their report, the Standing Committee on Justice and the Solicitor-General stated the government should prepare a vigorous program to convince the private sector to develop privacy codes and that both the Departments of Justice and of External Affairs should submit a Report to Parliament within eighteen months of the tabling of the



The author(left) in converstation with former MP Ged Baldwin, one of the architects of Canada's freedom of information and privacy legislation

Report, reporting to what extent the private sector has developed codes. The message is clear: if the private sector cannot do this on their own, then the Federal Government should step in.

The Committee further recommended that certain privacy rights be extended to the federally-regulated private sector, including the banks, airlines, telecommunications industry and others. Specifically, they recommend that the right found in "Sections 4 to 9 of the *Privacy Act* (fair information practices) and 12 to 17 (individual rights of access to data) and 29 to 35 (a mechanism for the Privacy Commissioner to receive and investigate complaints) be extended to the federally-regulated private sector by means of a separate part of the Act."

The Committee also recommended "that the Privacy Commissioner be empowered to review and approve implementation schemes developed by organizations in the federally-regulated private sector to comply with the *Privacy Act*. He should also be authorized to report to Parliament on the degree of progess in developing satisfactory data protection plans in the same sector."

Another criticism levelled at the Committee's Report, by Bill Loewen of Comcheq Services, was that there are no penalties for violations of any privacy principles. He felt that the Privacy Commissioner's role, as recommended by the Parliamentary Committee, is too limited. He recommended there be civil remedies against abusers available to the citizen, through recourse to the courts.

This question of the role of the Privacy Commissioner is fundamental to the privacy debate in Commonwealth countries. Canada has developed a unique system in creating a Commissioner who is an officer of Parliament with quasi-judicial powers and can do extensive investigations when a complaint is received or do spot checks on government departments to determine if they are complying with the law. The Privacy Commissioner, like the Information Commissioner, cannot overturn the decision of the head of an agency. This is based on the concept of ministerial responsibility, which says that the Minister is responsible to Parliament and Parliament alone. It would be anathema in our system of government to create an official who would have the power to overturn the decisions of Ministers. However, if a complainant is not satisfied with a decision rendered by the Commissioner a complaint can be laid with the Federal Court.

In contrast, Australia, in enacting her *Freedom of Information Law* in 1982, opted for a different system. There, a complaint can be laid with the Federal Ombudsman, if the request is taking too long or the complainant feels other administrative principles are being violated. In the event of denial of information a complaint can be laid with the Administrative Appeals Tribunal. This body can only recommend the release of documents but if a minister overturns the decision of the Tribunal he or she must submit the reasons before Parliament within thirty days.

New Zealand also allows complaints to the Ombudsman who can only recommend release. The *Official Information Act*, amended in 1987, calls for the full Cabinet to review a decision by the Ombudsman for the release of a document. Both Australia and New Zealand are thus incorporating within their parliamentary systems aspects of administrative law found in European and Scandinavian countries as opposed to Westminster-style governments. Quebec's Access law is unique in this respect in that their Access to Information Commission (composed of a Chairman and two Commissioners) has the power to direct disclosure of a document thus overriding the decision of a head of an institution.

These appeal mechanisms are important to the privacy debate as they will determine the future efficacy of laws that appear to be inevitable. It is certain that Parliament will adopt some of the measures recommended by the Parliamentary Committee as the move today towards greater privacy protections takes hold. Australia has introduced a Privacy Act in their Parliament (for the public sector only, for the moment) but, along with New Zealand, is also considering wider privacy protections in all sectors of society. All the democracies are, to some extent, involved in the privacy debate and developing some forms of protection. There have been enough voices raised to make this a reality.

The essence of the debate will become the methods which should be used to achieve these purposes so that the rights of the individual are protected while at the same time the state is not given extensive powers to intrude into the lives of individuals in the name of protecting their privacy.