Personal Information and the Protection of Privacy 1995

1995 Quebec, QC

Civil Section Documents - Personal Information and the Protection of Privacy

By: Denis C. Kratchanov, Counsel,
Information Law and Privacy Section
Department of Justice Canada

[See 1995 Proceedings at page 46]

Acknowledgements

The author wishes to thank Mr. Tom Onyshko, Mr. John Gregory, Mr. Colin H.H. McNairn, Mr. Jacques Dufresne, Mr. Gerald Taggart and Mr. Douglas Moen for their comments and suggestions. The author is particularly grateful to Mr. Tom Onyshko, who provided material from his forthcoming thesis on this subject.

The opinions expressed in this paper do not necessarily reflect the views of the Department of Justice Canada.

Table of Contents

FOREWORD

The purpose of this discussion paper is to identify principles that could serve as the basis for a Uniform Act on the Protection of Privacy and Personal Information.

Since the Uniform Law Conference of Canada adopted in 1994 a *Uniform Privacy Act* that creates a tort for invasion of privacy, this paper is concerned with the development of guidelines for the adoption of data protection legislation. There is a greater need for

uniformity in legislation applying to the private sector, so the paper focuses on this area in particular.

The discussion paper sketches the historical background of the development of privacy law and discusses the legal context in which privacy now evolves. Data protection legislation is not a new phenomenon, so it is not hard to identify principles upon which to base the legislation. The real difficulty for the ULCC, if it decides to adopt this project, lies not in agreeing on what those principles should be, but in determining how they should be implemented.

INTRODUCTION

Recent surveys have consistently shown that Canadians consider the issue of privacy a critical one. According to the 1992 privacy survey done by Ekos Research Associates, for instance, about half of the Canadian public is extremely concerned about their privacy, while the great majority is at least moderately concerned, putting privacy on the same level as unemployment and the environment and clearly surpassing concerns about national unity.(1) This high degree of concern about privacy may be explained, as some sociologists have suggested, by the theory that people instinctively oppose the idea of having their actions monitored and wish to maintain some areas of life free from official scrutiny. (2) People value a certain "looseness" in social relations so the weight of records about an individual's past actions does not become overwhelming, and they worry that large systems that collect detailed information change the balance between the public at large and central institutions.

Privacy commissioners, privacy advocates, and the public are demanding widespread data protection regulation for the Canadian public and private sectors. The Information Highway Advisory Council, established by the Minister of Industry in 1994 to assist the federal government in developing and implementing a strategy for Canada's Information Highway, has taken a similar position. Workplace monitoring, surveillance, drug testing and data matching are emerging as important privacy issues in the context of human rights and labour relations.

Technology threatening privacy

The Privacy Commissioner of Canada, Bruce Phillips, and his provincial counterparts see an urgent need to develop a proper regulatory framework for the information highway because of the immense amount of personal information that will soon be travelling on it and because of the public and private partnerships emerging to build it. Sectoral codes, self-regulation, patchwork legislation and industry watchdogs are no longer sufficient, according to Mr. Phillips,(3) and it is time for nothing less than broad privacy legislation for government and business.

The Commissioner calls for new broadly applicable national standards to be crafted with one of the major principles being that any informational exchange involving the federal government with the private sector carries the full protection of the *Privacy Act*. He

suggests setting out in law fair information practice codes to govern the traffic of electronic information with the government having the role of overseeing and monitoring privacy protection.

Information Highway Advisory Council report

The Information Highway Advisory Council was established in the spring of 1994 to examine the technological and non-technological implications of building Canada's communications infrastructure. The Council will submit its final report to the Minister of Industry this summer, but it has already issued a number of recommendations for government consideration and action, including recommendations on privacy, access to information and equitable access, security, copyright and offensive content.

The final recommendations on privacy call on the government to develop and implement flexible framework legislation to protect personal information in both the public and private sectors. The Council recommends that this legislation be based on the Canadian Standards Association Model Privacy Code.

Domestic and international pressures

Another factor creating pressure for governments to regulate is the new standard set by Quebec in legislating its private sector. Quebec is the first jurisdiction in North America to attempt to regulate data protection in its private sector. Despite initial opposition to regulation, companies now seem to be complying with the data protection requirements of the Act without great difficulty. Some companies are even extending these requirements to their businesses located outside Quebec, using privacy protection as a marketing tool.

There is also international pressure to consider regulation. The European Union privacy directive has been approved in principle by the Council of Ministers and is now under study by the European Parliament's Legal Affairs and Citizens' Rights Committee. The directive will have implications for Canada because of the provision allowing member countries to block the flow of data across borders to countries that do not have adequate data protection rules. If Canada does not develop regulations, the directive could act as a non-tariff trade barrier.

I. HISTORICAL BACKGROUND

Absolute privacy, except for the individual living alone on an island, has never existed. In the small towns and villages where most people lived before the industrial revolution, there was little or no privacy.(4) The details of one's wealth or health could not be hidden for long from other community members. Indeed, someone seeking privacy from the others might have been looked at with suspicion.

The industrial revolution and the large cities it created changed all that. With the industrial age, came individualism, anonymity and privacy.(5) More people became more mobile, moving where they could find work. The telephone and radio communications made the

limits of time and space less and less relevant. Gradually, the small communities where everyone knew everyone else began to disappear. The state had not yet attained the size, and it did not have the resources or the will, to collect much personal information about its citizens, and what little information there was had not yet acquired a high enough value to trigger the interest of the burgeoning large corporations. Individuals therefore came to enjoy, and to expect, an unprecedented level of privacy.

The same industrial age that allowed privacy to flourish, however, created the means to intrude upon it and eventually threaten to take it away. Progressively, with the introduction of income tax and with the creation of social programs, the state began to collect more and more personal information. The creation of the computer to process all this new information made information useful for new purposes, and it quickly gained in economic value. As workers are being replaced by computer-controlled machines and as new communications technologies have linked together not only the great financial capitals of the world, but also the most remote places on Earth, information and knowledge have gained a new importance in our economies. With computer technology, information can now be compiled, processed, stored, retrieved and communicated at speeds and in quantities unimaginable not long ago.

Widespread concern about privacy and the computerization of personal information first arose in the United States in the 1960s. Over that decade, the public and private sectors made new demands for personal information and tried to establish large computerized data banks. In addition, there were proposals to establish a national data centre that would bring together different types of personal information held by the U.S. government in a central data bank. Throughout the 1960s and into the early 1970s, congressional hearings, government studies, academic publications and popular books considered the new threats to privacy.

The issue of privacy in an information-based economy first attracted attention in Canada in the early 1970s when the former Department of Communications and the Department of Justice put together a joint Task Force on Privacy and Computers. The study produced by the Task Force warned that computers "may magnify, or at least highlight the problems" all information systems pose to privacy.(6) Today, with solitary mainframe computers having been replaced by powerful personal computers linked in networks, such a warning sounds like an understatement. And as the packaging of information by computers has improved over the years, so has the threat that it could be misused and that information about individuals might be used for purposes not originally intended.(7)

Since that study was published, the issue of privacy has slowly risen in importance as Canadians have realised that the privacy they thought they enjoyed in a post-industrial society is being eroded. In this new economy, information has become a commodity, and the public is calling out for protection and definition of ownership rights. (8)

II. LEGAL CONTEXT

Not surprisingly, the legal definition of privacy has evolved through time. In a 1888 textbook, Judge Thomas Cooley used the expression "the right to be let alone" in the context of immunity from the threat of physical harm.(9) This expression was quickly taken up in a 1890 article by two jurists concerned about the invasion of privacy that could be caused by photographic images.(10) In a now-famous article in 1890, Samuel Warren and Louis Brandeis argued for the creation of a general right of privacy that would give an individual a right to prevent the unauthorized use of private matters by the press. The authors foresaw that new technologies, such as the telephone and photography, would bring more violations of the right to be let alone, and they concluded that privacy protection required better legal protection. They also foresaw that private individuals would apply to the courts to prevent the sale and publication of photographs without their authorization.

Their prediction was quickly confirmed in 1902 when a New York Court held that the use of a photograph in an advertisement without the consent of the subject was actionable.(11) New York State then became the first of many jurisdictions to adopt privacy laws prohibiting the unauthorized use of photographic images for commercial purposes.(12)

In 1967, a more modern and more comprehensive definition of the right to privacy was proposed by professor Alan Westin, and it has since received general acceptance and has even been accepted by both the Supreme Court of Canada(13) and the United States Supreme Court.(14) The right to privacy is the "claim of individuals, groups and institutions to determine for themselves when, how and to what extent information about them is communicated to others."(15) In other words, privacy would be the "the right to exercise some measure of control over information about oneself."

In Canada, the right to be let alone is reflected in our laws in two ways. First, at the constitutional level, the *Canadian Charter of Rights and Freedoms*, while it does not contain an express right of privacy, does guard against unreasonable invasions of privacy. As the Supreme Court of Canada recognized in a 1990 decision, the primary value served by section 8 of the Charter (the right to be secure from unreasonable search or seizure) is privacy.(16) The Supreme Court has thus established a constitutional right to privacy, (17) although exclusively in the criminal law context, with respect to the seizure of bodily fluids (18) and the electronic surveillance of individuals;(19) it seems more reluctant to do so with respect to personal information stored in data banks.(20) Since other decisions by the Court have interpreted section 8 in a more relaxed fashion in relation to administrative law, the level of constitutional protection given to personal information may in fact be limited.(21)

Section 7 of the Charter may also contain a residual right of privacy, but this remains essentially an untested theory,(22) since the Supreme Court seems reluctant to make more than vague pronouncement on the matter. In any case, the Charter is essentially an instrument for checking the powers of governments over the individual, so this constitutional right to privacy would apply only to state action and not to private conduct. (23)

On the other hand, some common law provinces have adopted legislation establishing a tort liability for invasion of privacy. These provinces are British Columbia,(24) Saskatchewan, (25)Manitoba(26) and Newfoundland(27). The provincial Privacy Acts creating a tort have not generated much judicial consideration(28), however, and they have been difficult to enforce.(29)

In Quebec, privacy rights are protected at three different levels. First, section 5 of the *Charter of Human Rights and Freedoms*(30), an Act of a quasi-constitutional nature, recognizes a broad right of privacy by stating that "every person has a right to respect for his private life," and it further provides for a right to compensation for a prejudice resulting from an interference with that right. The *Civil Code*(31) then complements the Quebec Charter by defining what constitutes an invasion of privacy and limiting the right of persons to collect, use and disclose personal information on another person. Both statutes are binding on public and private entities, as well as on individuals, and both provide a right of action to persons whose privacy rights have been infringed. (The third level of privacy protection, comprehensive data-protection, is discussed below.)

In the late 1980s and early 1990s, the Uniform Law Conference of Canada began work to adopt a Uniform Protection of Privacy Act that would have recognized a tort of invasion of privacy. The Act was adopted by the Conference in 1994.(32)

The definition of the right of privacy as the right to exercise some measure of control over information about oneself has led most countries of Western Europe(33) to adopt what is now referred to as data protection legislation. With respect to the public sector at least, the United States(34) and Canada have done so as well.

In Canada, the federal *Privacy Act* (35), enacted in 1982 and replacing Part IV of the *Canadian Human Rights Act*(36), governs the collection, use, disclosure, retention and disposal of personal information by federal government institutions, which includes all federal departments, most federal agencies and some federal Crown Corporations. The *Privacy Act* is not the only statute protecting personal information held by the Government of Canada, however. Certain categories of personal information receive fuller protection under such statutes as the *Income Tax Act*(37) and the *Statistics Act* (38)

Most provinces now also have data protection legislation similar to the federal *Privacy Act* to apply to their public sectors: British Columbia,(39) Alberta(40), Saskatchewan(41), Ontario(42), Quebec(43) and Nova Scotia(44).

Quebec is the only province to have adopted comprehensive data protection legislation applicable to the private sector(45). That legislation provides a detailed framework for implementing the *Civil Code*'s provision for the collection, use and disclosure of personal information. The legislation came into force in January 1994, and while it may still be too early to fully assess its results, both expected and unexpected, it is fair to say that it has not created havoc for Quebec businesses.

That is not to suggest that use of personal information by the private sector outside Quebec is completely unregulated. But privacy protection in the Canadian private sector consists of

a patchwork of laws, regulations and codes that create different standards applying to few industries.

The *Criminal Code* (46), for instance, makes it a criminal offence to intercept a private communication. In the telecommunications industry, the Terms of Services of telephone companies approved by the CRTC include a provision on the confidentiality of client records. The public outcry that followed the introduction of the caller identification service led the CRTC to force telephone companies to offer free per-call blocking and line-blocking for those with particular need. The *Telecommunications Act* (47), for its part, now recognizes privacy in the telecommunications industry as a fundamental principle. It applies only to federally regulated carriers, however, and not to telecommunications resellers or to information service providers. In the banking industry, section 459 of the *Bank Act* (48) allows the government to regulate a bank's use of information obtained from its customers. Draft regulations were prepared for the Standing Senate Committee on Banking, Trade and Commerce in 1993, but they have not been adopted by the government. The Canadian Bankers' Association has, however, adopted a model privacy code, which has led individual banks to set out their own privacy codes. In the insurance sector, the Canadian Life and Health Insurance Association adopted Right to Privacy Guidelines, and the Insurance Bureau of Canada has adopted its own Model Privacy Code. In addition, at the provincial level there is credit-reporting legislation, such as Ontario's *Consumer Reporting Act*(49).

III. PRINCIPLES FOR DATA PROTECTION

The data protection acts referred to above, whether they apply to the public or private sectors, or to both, embody principles which were adopted by the OECD in 1980 in the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Information*. These Guidelines were developed to help harmonise national privacy legislation and, at the same time, prevent interruptions in international flows of data (50). Canada formally adhered to the Guidelines in 1984, committing the federal government to the protection of personal privacy in both the public and private sectors. At the centre of the OECD Guidelines are eight principles of fair information practices (see Annex 1). These eight principles are the foundation upon which privacy legislation has been based, whether it is directed at the public or private sectors. To follow up on the commitment it made when it subscribed to the OECD Guidelines, the federal government undertook to encourage private sector corporations to develop and implement voluntary privacy protection codes.

Since there is already privacy legislation embodying the OECD Guidelines in the public sector at the federal level and in most provinces, the area where there is the most need for privacy legislation guidelines is the private sector.

The federal government has been working closely with the Canadian Standards Association (CSA), which has begun to draft a Model Privacy Code that would meet or surpass the OECD Guidelines while balancing trade interests and business needs with the consumer's inherent right to privacy. The CSA has brought together representatives from consumers groups and

unions, the transportation, telecommunications, insurance, health and financial services industries, public sector officials and other general interest groups.

The final version of the Model Code should be adopted by the CSA in the fall of 1995, but a draft version has already been circulated for public comments (See Annex 2). It is the most up-to-date set of guidelines on the protection of personal information in the private sector and one of the most useful tools available to establish guidelines for privacy legislation. The Information Highway Advisory Council has called on the federal government to adopt legislation that would require sectors or organizations to meet the standards of fair information practices contained in the CSA model code.

At the core of the Draft Model Code are 10 interrelated principles for the protection of personal information:

1. Organizations are accountable for the personal information they collect.

2. Organizations should identify the reasons for collecting personal information.

3. Individuals are required to consent to the collection, use and disclosure of personal information.

4. Collection of information should be limited.

5. Use, disclosure and retention of information should be limited.

6. The information collected must be accurate.

7. There must be safeguards to protect information.

8. Organizations' policies and practices must be open.

9. Individuals have a right of access to their own information.

10. An individual can challenge an organization for not complying with the above principles.

These principles, which in one form or another should be in any data protection legislation, could be complemented by additional measures in related areas. Following the lead of the United Kingdom, the legislation might provide individuals with a right of action for harm caused by inaccurate personal information, loss of personal information, or unauthorized destruction of personal information(51). In addition, legislation might recognize the central role of technology by requiring assessments of new technologies for privacy implications before they are implemented.(52)

IV. IMPLEMENTATION

The adoption of legislation is not a panacea to all the ills in society. For a time, governments may have believed that by adopting legislation they could regulate not only the market imbalances created by monopolies, but also a whole sector of activities to ensure that they provided adequate service to citizens. In an open economy, however, the markets and the

law of supply and demand regulate economic activities. Since the deregulation of the American airline industry in the late 1970s, governments have tried to regulate less but to regulate better. In Canada, whole sectors of activities have been deregulated in the last 15 years. This trend is continuing, as shown by the introduction in Parliament last year of a bill (the *Regulatory Efficiency Act*) that would allow the replacement of regulations by standards negotiated between a responsible minister and a regulated entity. Whether that bill is passed or not, the trend is well established: governments will look at legislation and regulations only when other methods of controlling an activity or a behaviour have failed.

That is not to say, however, that the adoption of data protection legislation applicable to the private sector should be precluded. Privacy is a human right protected under the *Canadian Charter of Rights and Freedoms*, and similar human rights, such as equality rights, benefit as well from protection in other legislation. The same reason that lies behind legislation against discrimination or supporting workplace safety or environmental protection applies to a right of privacy: to protect a societal value that is fundamental to the interest of all citizens.

Privacy, as a subject of legislation, is not exclusively either a federal or provincial concern. It is an area of shared responsibility, like human rights legislation, and legislation in this area should preferably be, if not identical throughout the country, at least based on the same underlying principles, especially with respect to the private sector. Given the ease with which information crosses boundaries, cooperation between the federal and provincial governments on this issue is essential if we are to meet the concerns that Canadians have expressed over privacy.

Data protection legislation can take many forms, but to be effective it needs to be based on a set of fair information practices similar to the 10 principles enunciated in the CSA Draft Model Privacy Code. The difference lies in the degrees of coercion and voluntary cooperation it relies on. A "light" version would require collectors and users of personal information to adopt privacy codes, based on the CSA model, within a specified time frame. An advisory body could help draft and promulgate the code, and the legislation would impose codes created by that body if the deadline has not been met. Compliance with the codes would be purely voluntary. A "heavier" version would provide a public body with the powers to force a private sector entity to comply with its own code(53). Between the two versions, there is a range of "medium" versions that could be developed.

Another variation of the two options outlined above could be to design codes that are sector specific, which would allow greater flexibility to the protection of privacy interest in different contexts. Having separate data protection laws or regulations to address the concerns of specific industries such as telecommunications and insurance, might cause severe difficulties in compliance, however, since different sectors of industry exchange information(54) and the lines between industries are beginning to blur.

CONCLUSION

The adoption of data protection standards for both the private and public sectors is a goal worth pursuing. The inclusion of such standards in legislation, even without strong coercive measures, would provide an incentive to both the public and private sectors to give personal information the protection it deserves. This legislation could also help Canada meet privacy standards that are being set by its trading partners in Europe. Data protection laws have been in existence in Europe and in Canada for many years, and are now familiar to Canadians. They are not intended to prevent businesses or governments from collecting and using the personal information they need to conduct their business, but to give back to citizens some control over what is known about them by others.

The first step for the ULCC, if it decides to deal with this issue, is to agree on the principles that a data protection law should promote. These might be the principles identified in the CSA Draft Model Privacy Code; in any event, they should be consistent with the OECD Guidelines. The second step would be to decide on the best approach to ensure compliance with those principles, i.e. "light" or "heavy" legislation. The third and final step would be to prepare draft legislation that would be available to any government in Canada. The ULCC can play a vital role in ensuring that legislation adopted in this area by Parliament and the provinces does not lead to confusion in the marketplace for consumers and businesses alike or to the creation of new non-tariff barriers between provinces.

ANNEX 1: OECD GUIDELINES

Basic Principles of National Application

Collection Limitation Principle

1. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

2. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

3. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

4. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

5. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

6. 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 identify and usual residence of the data controller.

Individual Participation Principle

7. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

i) within a reasonable time;

ii) at a charge, if any, that is not excessive;

iii) in a reasonable manner; and

iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

8. A data controller should be accountable for complying with measures which give effect to the principles stated above.

FOOTNOTES

1. Ekos Research Associates Inc., *Privacy Revealed*, Ottawa, 1993, p.4. More recently, a 1994 Gallup Canada survey indicated that more than 80 percent of Canadians were

concerned about personal information about them that might be collected by companies involved in the Information Highway: Gallup Canada, *The Information Highway*, Andersen Consulting Canada, 1994; a Louis Harris & Associates survey conducted in the fall of 1994 confirmed that the privacy issue in Canada continues to be concern to a large majority of the public: Louis Harris & Associates, *The Equifax Canada Report on Consumers and Privacy in the Information Age*, Anjou, Equifax Canada Inc., 1995, 59 p.

2. James B, RULE et al., *Preserving Individual Autonomy in an Information-Oriented Society, in Computers and Privacy in the Next Decade*, ed. by Lance J. HOFFMAN, New York, Academic Press, 1980, pp.65-87.
3. Privacy Commissioner of Canada, *1993-1994 Annual Report,* Ottawa, Canada Communications Group, 1994, pp. 5-6.
4. Jeremy RIFKIN, *Biosphere Politics,* New York, Harper Collins, 1992, p. 154.
5. Louis NIZER, *The Right of Privacy, a Half Century's Developments,* (1940-41) 39 Mich.L.R. 526.
6. Task Force on Privacy and Computers, *Privacy and Computers*, Ottawa, Information Canada, 1972.
7. Examples of such misuse of personal information abound. A recent one in British Columbia involved a police officer who, by using the license plate numbers of cars parked in front of a health clinic performing abortions, obtained access, by using the Province's computerized motor vehicle database, to the names and addresses of staff members at the clinic. These staff members then received phone calls and mail at home from anti-abortion groups. See Investigation reportP95-005, March 31, 1995, Information and Privacy Commissioner of British Columbia for a discussion of the general issues surrounding privacy in a complex multi-user database.
8. Anne Wells BRANSCOMB, *Who Owns Information?*, New York, BasicBooks, 1994, p. 1.
9. Thomas COOLEY, *A Treatise on the Law of Torts or the Wrongs which arise independent of contract*, 2nd ed. (1888) p. 29.
10. S. WARREN and L. BRANDEIS, *The Right of Privacy*, (1980) 4 Harv. L. Rev. 193.
11. *Robertson v. Rochester Folding Box Co*,. (1902), 171 N.Y. 538.
12. 1903 N.Y.L.C. 132, Sec. 1,2.
13. R.*v. Duarte*, [1990] 1 S.C.R. 30,46.
14. *U.S. Department of Justice v. Reporters Committee for the Freedom of the Press*, (1989) 489 U.S. 749. The case dealt with an access to information request for personal information made under the U.S. *Freedom of Information Act*.
15. A. WESTIN , *Privacy and Freedom,* New York, Atheneum, 1967, p.32.
16. *R. v Duarte,* [1990] 1 S.C.R. 30,43.
17. The Supreme Court of the United States had recognized a constitutional right to privacy in 1967 in its decision in *Griswold v. Connecticut,* (1967) 381 U.S. 479.
18. *R. v. Dyment* [1988] 2 S.C.R. 417; R.Collaruso [1994] 1 S.C.R 20.
19. R. *v. Duarte*, [1990] 1 S.C.R. 30 (interception of private communications); *R. v. Wong,* [1990] 3 S.C.R. 36 (video surveillance) and *R. v. Wise*, [1992] 1 S.C.R. 527 (installation and monitoring of a tracking device on a vehicle)>
20. *R. v. Plant* [1993] 3 S.C.R. 281: the Court ruled that the police's warrantless obtention, from the hydro Commission, of the records showing the electricity consumption of the defendant did not violate section 8 as these records were not

"confidential". The Court did not forclose, however, the possibility of a section 8 claim with respect to records prepared in a commercial context. (See, however, the stong dissent of Ms. Justice Mclaughlin).

21. *R. v. McKinlay Transport Ltd*., [1990] 1 S.C.R. 627: The Court ruled that, at least vis-a-vis the Department of Revenue, a taxpayer right to privacy with respect to financial records was relatively low.
22. See, for example the comments of Mr. Justice La Forest in *R. v. Beare*, [1988] 2 S.C.R. 387, at 412 and those of Chief Justice Dickson in *R. v. Morgentaler*, [1988] 1 S.C.R. 30, at 56.
23. *McKinney v. University of Guelph*, [1990] 3 S.C.R. 229.
24. *Privacy Act*, R.S.B.C. 1979, c. 336.
25. *Privacy Act*, R.S.S. 1978, c. P-24.
26. *Privacy Act*, R.S.M. 1987, c. P-125.
27. *Privacy Act*, R.S.N. 1990 .P-22.
28. Ian LAWSON, *Privacy and Free Enterprise*, Ottawa, Public Interest Advocacy Centre, 1992. p. 74.
29. Georges S. TAKACH, *Law in the Digital Age: A Tour d'Horizon, in Heading into the Information Age,* Proceedings of a Conference organized by the Canadian Bar Association and the Common Law Section of the Facutly of Law of the University of Ottawa, May 16, 1995, p. 11.
30. R.S.Q., c, C-12.
31. S.Q. 1991, c. 64.
32. The proceedings of the 1994 meeting had not yet been published at the time of the completion of this paper in June 1995.
33. The first European countries to adopt data protection legislation applicable to both the public and private sectors were Germany, France, Austria and Sweden in the 1970s. To harmonize legislation within the European Community (E.C.) and to prevent that data transfers between member countries might be blocked by national data commissioners, the E.C. has been working since 1990, on the adoption of data protection directive. This directive may, however, have the effect of preventing the transfer of personal data to non-member countries that do not provide an acceptable level of protection to personal information.
34. The federal *Privacy Act*, passed in 1974, protects personal information contained in records of the federal government.
35. R.S.C. 1985, c.P-21.
36. S.C. 1976-77, c. 33.
37. R.S.C. 1952, c. 148, as amended by S.C. 1970-71- 72, c. 63 (as amended).
38. R.S.C. 1985, c. S-19. s. 17.
39. *Freedom of Information and Privacy Act, S.B.-C. 1992, c. 61.*
40. *Freedom of Information and Privacy Act, S.A. 1994, c. F-18.5.*
41. *Freedom of Information and Privacy Act, S.S. 1990-91, c. F-22.01*and the *Local Authority Freedom of Information and Protection Act*, S.S. 1990-91, c. L.-27.1.
42. *Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31* and the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56.

43. *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, R.S.Q., c. A-2.1.
44. *Freedom of Information and Protection of Privacy Act,* S.N.-S. 1993, c. 5.
45. *An Act Respecting the Protection of Personal Information in the Private Sector*, S.Q. 1993, c.17.
46. R.S.C. 1985, c. C-46, sec.183-196.
47. S.C. 1993, c. 38, s.7.
48. R.S.C. 1985, c. B-1
49. R.S.O. 1990, c. C.33.
50. OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Information, 1980,* p.5.
51. *Data Protection Act*, 1984, ss. 22- 24.
52. In this regard, see recommendation 7.7 of Parlimentary Committee which reviewed Canada's *Privacy Act* in 1987: Standing Committee on Justice and the Solicitor General, *Open and Shut: Enhancing the Right to Know and the Right to Privacy,* Ottawa, Department of Supply and Services, 1987, p.78.
53. The importance of an independent privacy commissioner's office has been emphasized in some of the literature on data protection. In a study of the implementation of data protection legisltion in five countries, professor David H. Flaherty (now the Information and Privacy commissioner of British Columbia) argued that the success of such legislation depended on whether there was an independent agency chared with administering it: David H. FLAHERTY, *Protecting privacy in surveillance Societies: The federal republic of Germany, France, Canada and the United States,* Chapel Hill, University of North Carolina Press, 1989, pp. 381-85.
54. Georges S. TAKACH, *Law in the Digital Age: A Tour d'Horizon,*in *Heading into the Information Age,* Proceedings of a Conference organized by the Canadian Bar Association and the Common Law Section of the Faculty of Law of the University of Ottawa, May 16, 1995, p. 11-12,