JC
599
C2
J43
1989

Industry Canada
LIBRARY
JUL 07 1998
BIBLIOTHÈQUE
Industrie Canada

THE PANOPTIC SOCIETY:

PRIVACY AND INFORMATION SERVICES IN CANADA

COMMUNICATIONS CANADA
OCT 21
LIBRARY — BIBLIOTHÈQUE

M. Sharon Jeannotte
Strategic Policy Planning Division (DSP)
Department of Communications

January 1989

TABLE OF CONTENTS

> ... the Panopticon is a building of circular structure with a series of individual cells built around a central "well"; at the center is an inspection tower from which each of the cells could be observed and monitored. A calculated illumination of the cells, along with the darkening and masking of the central tower, endows the "introspective force" with "the unbounded faculty for seeing without being seen".[1]

1. Introduction

According to civil libertarians, information technologies have provided the means of realizing Jeremy Bentham's intellectual vision of the Panopticon. They claim that we are now living in a society where massive amounts of information can be collected by government agencies and commercial organizations, then stored, manipulated and used without the individual's knowledge or consent. Moreover, they contend that there are few, if any, avenues of recourse open to individuals who feel that their privacy has been abused through misuse of information in electronic form.

The purpose of this document is to examine the issue from a public policy viewpoint, as background to a discussion paper on information services which is being prepared by the Strategy and Plans Branch of the Department of Communications. That paper will focus on the market for advanced information services in Canada, the potential threats and opportunities inherent in the widespread development and use of these services and the adequacy of current policies to achieve Canadian objectives.

As part of the overall exercise, this background paper will trace the evolution of the privacy issue, review public and expert opinion on the subject and examine some of the major concerns about misuse of information services. It will look at the current state of privacy protection in Canada, with particular emphasis on recent developments at the federal level. It will then draw some conclusions and suggest various options for action in Canada, including steps that the Department of Communications should take to address the privacy issue.

Volumes have been written over the past twenty years or so

---

[1] Kevin Robins and Frank Webster, "Cybernetic Capitalism: Information, Technology and Everyday Life" in The Political Economy of Information. Edited by Vincent Mosco and Janet Wasko. Madison: The University of Wisconsin Press, 1988, p.57. The Panopticon is a philosophical construct devised by Jeremy Bentham at the end of the 18th century and intended as the ultimate illustration of the architecture of control.

on the threats to privacy posed by information technologies. This review will therefore, of necessity, be a brief condensation of the major elements of this complex and controversial issue. The reader should consult the references for a more in-depth treatment of specific topics.

1.1 Definition of privacy

Paradoxically, while the issue of privacy arouses strong reactions in among individuals and within organizations, there has been no general agreement about the definition of privacy that should apply in public policy discussions. However, one definition has been gaining currency and is used as a starting point for several of the most influential treatments of the subject. It is taken from Alan Westin's Privacy and Freedom and will serve as the working definition for this paper as well:

> Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.[2]

In 1987, the Standing Committee on Justice and Solicitor General recommended that this definition be added to Canada's Privacy Act to facilitate implementation and interpretation.[3] In its response to the Standing Committee, the federal government rejected this approach, preferring to restrict the scope of the Act to what is being protected -- "personal information" as itemized in thirteen-point descriptive list. The concept of privacy, therefore, remains ill-defined and vague in Canada's foremost legislation on the the subject.

1.2 Evolution of the privacy issue

Because of definitional problems, privacy, like beauty, is often in the eye of the beholder. Depending on the commentator's political, social or economic biases, privacy in an information-based society is either one of the most profound threats to human liberties or a "nuisance" issue designed to restrict the freedom of the information marketplace. Perceptions about privacy have shifted as the tides of other social attitudes have swung from left to right over the past two decades. For governments, this has meant finding that point in the political spectrum that balances the right of access to information with the right to

---

[2] Alan Westin, Privacy and Freedom. New York: Atheneum, 1967, p. 39.

[3] Standing Committee on Justice and Solicitor General, Open and Shut: Enhancing the Right to Know and the Right to Privacy. Ottawa: Queen's Printer for Canada, 1987, p. 58.

personal privacy.

On the economic front, the telecommunications and cable industries, as well as other information service providers, have been eloquent defenders of the need to balance privacy concerns against other societal goals:

> It is important to underscore an important aspect of that system [the American political system] in the light of privacy policy: the rationalizing ideology which dominates the discussion of privacy. That ideology can be summed up in one word `balance'. The term means that privacy is one of many valuable goals, and that its pursuit, while worthy in itself, must not cause other highly valued goals to be forgone in the process. These other goals include safeguarding and husbanding economic investments, promoting governmental efficiency, and protecting society.[4]

On the other hand, civil libertarians, such as the Canadian Privacy Commissioner, are quick to point out that "computer matching ... carried on in the name of efficiency, good government and law enforcement makes it potentially a more, not less, dangerous instrument in the state's hands".[5]

There is some evidence to suggest that this tension of interests played a key role in the evolution of the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data". The OECD Guidelines (discussed in greater detail in a later section of this paper) are a set of recommendations for minimum standards for the treatment of personal data which has formed the backbone of voluntary data protection codes adopted by the private sector in OECD countries. A doctoral thesis done for York University in 1988 and based on personal interviews with the principals in the drafting of the OECD Guidelines concluded that:

> The issues which initially arose in the international computer/communications question were wide ranging. As argued above, most of these initial questions were national in perspective and state-centric in motivation. By bringing the issues to the OECD, not only were policies harmonized, but harmonized in the

---

[4] James E. Katz, "U.S. telecommunications privacy policy: Socio-political responses to technological advances", Telecommunications Policy. (December 1988), p. 357. (The author is an employee of Bell Communications Research.)

[5] John Grace, Annual Report, Privacy Commissioner, 1983-84. Ottawa: Minister of Supply and Services, 1984, p. 4.

> liberal international market framework. The organizational processes described brought academics and state officials who were theorizing about the "information age" in the European context more directly in contact with both state representatives from more liberal countries and those from dominant transnational economic groupings. Privacy protection had become a damage control exercise for some people, rather than the control of the new technology envisaged by early analysts. Thus, the organization served to integrate dominant economic groups with the process and resultant content of a policy ideology of the information age.[6]

Politics is the "art of the possible", and public policy will have to continue to seek accommodation between these contending forces. In the 1980s, as subsequent sections will illustrate, the balance appears to have shifted toward the market forces. In the 1990s, the pendulum may begin to swing back to the civil libertarians, if polling data suggesting increasing public concern about social issues is to be taken as the leading edge of a trend line.

1.3 Public opinion

Does the public perceive invasion of privacy via information technologies as a serious problem? Polling results suggest that it does, although tracking the issue is not an exact science because of differences in sample sizes, questions and techniques among the surveys that have been done. The following is a summary of the results.

Canadian attitudes

DOC - 1970-71

An attitudinal survey done in for the Department of Communications in winter 1970-71 included a question which asked 1000 Canadians if computers threatened personal privacy. Thirty-seven per cent agreed while 41 per cent disagreed. These results were roughly comparable to those derived from an American survey done about the same time which found that 38 per cent of respondents agreed that computers represent a real threat to people's privacy, while

---

[6] Stephen D. McDowell, Hegemony and International Organizations: A History of Transborder Data Flow Research Programmes. North York, Ontario: Graduate Programme in Political Science, York University, March 1988, p. 166.

54 per cent disagreed.[7]

Ontario Ministry of Transport and Communications - 1981

A sample of 1086 Ontario residents were asked to indicate the importance of thirteen issues associated with microelectronics. The number one concern was privacy and confidentiality of information cited by 63 per cent of respondents. The number of people controlling information was third at 45 per cent. Asked to speculate on who would invade their privacy electronically, the results were:

- credit rating agency - 58 per cent
- computer or data bank - 55 per cent
- insurance company - 51 per cent
- provincial government - 52 per cent
- federal government - 52 per cent
- bank - 50 per cent

Bell Canada - June 1981

Bell asked a representative sample of Canadians about their concerns regarding computer-based technology. Storage of personal information on computers was cited by 64 per cent.

Ontario Ministry of Transportation and Communications - 1983

Probably the most comprehensive survey of public attitudes to privacy and new information services was done in 1983 for the Ontario Ministry of Transportation and Communications. Unfortunately, the sample was limited to 210 households in London, Ontario and therefore cannot be considered statistically reliable in terms of projection to the general Canadian population. Nevertheless, the results are interesting because they explore the major parameters of attitudes to privacy in advanced information services in greater depth than any other Canadian survey.[8]

1) Importance of privacy relative to other issues (rated as very important or important):

---

[7] Department of Communications, Survey of public attitudes towards the computer. Ottawa: Information Canada, 1973, p. 8.

[8] The details in this section are quoted from Neil Vidmar, Privacy and Two-way Cable Television: A Study of Canadian Public Opinion. London: University of Western Ontario, May 1983, pp. 16-46. They should be considered indicative rather than absolute reflections of the distribution of attitudes within the Canadian population.

Inflation	-	96 per cent
Unemployment	-	94 per cent
Preventing crime	-	93 per cent
Protecting privacy	-	90 per cent
Stopping spread of nuclear weapons	-	78 per cent
Stopping strikes	-	69 per cent
Improving relations between Quebec and the rest of Canada	-	63 per cent

2) Perceived seriousness of various privacy invasions (serious to extremely serious):

RCMP taps phones	-	76 per cent
Use of medical records by insurance company without consent		69 per cent
RCMP opens mail	-	62 per cent
Magazine sells subscriber list	-	58 per cent
TV monitor in workplace	-	53 per cent
Government makes list of people attending political meeting	-	52 per cent
Stores share credit information		41 per cent
Cable company monitors customer viewing habit by computer	-	38 per cent

3) Public trust of government and private business to use personal information properly:

Federal and provincial governments:
- Trust - 51 per cent
- Worried - 49 per cent

Business and companies:
- Trust - 38 per cent
- Worried - 62 per cent

4) Perception of changes in privacy and concern about it:

- much more privacy than in past	-	2 per cent
- somewhat more privacy than in past	-	8 per cent
- about the same degree of privacy	-	22 per cent
- somewhat less privacy than in past	-	47 per cent
- much less privacy than in past	-	21 per cent

Concern about threats to personal privacy:

- very concerned	-	18 per cent
- somewhat concerned	-	44 per cent

- only a little concerned -26 per cent
- not concerned at all- 12 per cent

5) Attitudes to computers (agree or somewhat agree):

- save time and energy- 90 per cent
- take jobs away - 87 per cent
- pose a danger of personal privacy - 84 per cent
- too complicated to learn 29 per cent

6) Reactions to concept of two-way television (agree or somewhat agree):

- prefer to shop in person - 82 per cent
- cable company computer will have too much information about personal life - 80 per cent
- too costly - 79 per cent
- would tempt to buy too much - 60 per cent
- would be frequent user of two-way services - 54 per cent
- too complicated - 21 per cent

7) Potential privacy problems in two-way services:

A) Extent of caring whether people know personal buying or viewing habits:

an extremely private matter - 14 per cent
a private matter - 29 per cent
a somewhat private matter - 33 per cent
not a private matter - 24 per cent

B) Use of buying habit information about you and your family:

a very serious privacy invasion - 25 per cent
a serious privacy invasion - 36 per cent
a somewhat serious privacy invasion - 35 per cent
not an privacy invasion 4 per cent

C) Extent to which use of personal information for marketing purposes would deter individual from using two-way cable TV services:

definitely stop - 36 per cent
possibly stop - 57 per cent
not stop 7 per cent

D) Extent to which cable companies should tell

individual subscribers about collection and use of personal information:

a good idea - 91 per cent
not a good idea - 8 per cent
don't know - 1 per cent

E) Need for written permission before cable companies use personal information for marketing purposes:

a good idea - 96 per cent
not a good idea - 2 per cent
don't know - 2 per cent

F) Willingness to allow use of personal information by cable companies with advance notification:

yes - 43 per cent
no - 51 per cent
don't know - 6 per cent

Willingness to allow use of personal information in return for a 50 per cent reduction in cable rates:

yes - 57 per cent
no - 30 per cent
don't know - 13 per cent

G) Selling of personal information derived from two-way cable services to third parties: should it be forbidden?

yes - 91 per cent
no - 4 per cent
don't know - 5 per cent

H) Use of personal information derived from two-way cable services by the government or courts should be:

forbidden in all cases - 26 per cent
forbidden except in a few justifiable cases - 38 per cent
forbidden in most cases - 29 per cent
generally permitted - 7 per cent

G) Should there be strict regulation to minimize the possibility of illegal use of personal information (e.g. by employees of the cable companies or hackers)?

yes -	98 per cent
no -	1 per cent
don't know -	1 per cent

American attitudes

In the United States, a number of major surveys have been carried out by national polling organizations in the past few years on the subject of information technologies and personal privacy. Therefore, the data are somewhat more comprehensive and comparable than in Canada.

In 1985, the Office of Technology Assessment of the U.S. government commissioned a review of survey research on the subject, with the following results.

- Percentage perceiving computers as a threat to personal privacy:

  - 1974: yes - 38 per cent
    no - 41 per cent

  - 1977: yes - 41 per cent
    no - 44 per cent

---

[12] Goldfarb Consultants, The Goldfarb Report 1987, raw data from computer printouts, s.12, q.8.

- 1978: yes - 54 per cent
  no - 33 per cent

- 1983: yes - 51 per cent
  no - 42 per cent

- Percentage believing that personal information in computers is not adequately safeguarded:

  - 1978: 52 per cent
  - 1983: 60 per cent

- Percentage believing that each organization shares information about individuals with others (1983):

  - credit bureaus - 75 per cent
  - loan companies - 65 per cent
  - insurance companies - 57 per cent
  - welfare agencies - 51 per cent
  - Census Bureau - 51 per cent
  - banks - 51 per cent
  - public opinion research firms - 50 per cent
  - the FBI - 38 per cent
  - the IRS - 36 per cent
  - the telephone company - 33 per cent

- Percentage supporting potential federal laws on information abuse (1983):

  - federal law requiring double-checking of sensitive computer data - 92 per cent

  - federal law to make privacy invasion by information-collecting agencies a criminal offence - 83 per cent

  - impeachment of public officials violating privacy of individuals or groups without a court order or trial - 81 per cent

  - federal law punishing authorities responsible for making computer errors that hurt credit ratings, harm companies or endanger lives - 71 per cent

  - federal laws putting companies that shared information which violated the privacy of the individual out of business - 68 per cent

  - federal regulations on the kind of information that could be combined with other information to

produce individual profiles - 66 per cent[13]

It is evident that concern about privacy and advanced information technologies has been rising in the past decade in both Canada and the United States. This has sometimes been referred to as an issue without a constituency, since widespread public concern has not translated into a focus for action. The public opinion findings suggest, however, a growing sense of unease, as consumers discover there are side effects to information gathering activities that have generally operated outside the framework of public attention.

Certain parallels to the environmental protection issue are evident: the emergent right to privacy in an information-based economy may become as important to individuals as the right to a clean environment has become in a manufacturing-based economy. And there are hints in the American data supporting federal government intervention that the public will expect those who profit from the processing of "information resources" to assume responsibility for ensuring that consumers are not harmed by this activity.

1.4 Expert opinion

What do the experts say about privacy threats in electronic information systems? Are they more or less concerned than the general public? The following is a brief review of the major positions of privacy experts, both on the Canadian and the international scene.

Canadian experts

David H. Flaherty, Professor of History and Law, University of Western Ontario

Professor Flaherty is probably the leading Canadian expert on the privacy implications of advanced information services. His area of expertise is two-way services on cable, but his comments could apply to private sector

---

[13] U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Electronic Record Systems and Individual Privacy. (OTA-CIT-296). Washington: U.S. Government Printing Office, June 1986, pp. 26-31. Most of the information cited in this section is drawn from polls conducted by Louis Harris and Associates, Inc. -- The Dimensions of Privacy: A National Opinion Research Survey of Attitudes Toward Privacy (conducted for Sentry Insurance, December 1979) and The Road After 1984: A Nationwide Survey of the Public and Its Leaders on the New Technology and Its Consequences for American Life (conducted for Southern New England Telephone, December 1983).

companies offering information services on any medium.

> New York Attorney General Robert Abrams has argued that interactive cable television is going to generate "the single largest repository of personal data and information in the history of the world." If this allegation is correct, and there are compelling reasons to think that it is, then two-way services pose considerable challenges to individual privacy and the confidentiality of personal information. Companies offering interactive services must be encouraged to develop and implement provisions and guidelines on confidentiality and privacy that will limit the collection, storage and use of personal information to legitimate business purposes in such a manner that subscriber interests are protected at all times. Contrary to the customary practices of most private concerns, companies will have to be persuaded that there are appropriate limits on the uses of personal information that comes into their possession through the operation and use of two-way systems.[14]

Professor Flaherty is perhaps most noted for his development of the concept of "group privacy" which could be threatened by information derived from a source such as channel monitoring. Using statistics on neighbourhood viewing patterns, for instance, it would be possible for a marketer to develop a profile of the political, religious and sexual preferences of that group of people. He contends that the economic benefits to carriers of selling such information may prove to be an overwhelming temptation, and he believes that both self-regulation and legislative regulation will become necessary to control the practice.[15]

He suggests that companies should observe a number of practices to ensure the confidentiality of subscribers, including:

1) informed consent by subscribers in a written contract;

2) adherence to a code of fair information practices;

3) requiring all employees to sign a form concerning the confidentiality of subscriber lists;

---

[14] David H. Flaherty, Protecting Privacy in Two-Way Electronic Services. White Plains, N.Y.: Knowledge Industry Publications, 1985, p. 143.

[15] Flaherty, p. 149.

4) minimizing the amount of data collected and the time it is retained;

5) limiting the possibility of data linkage to develop profiles of subscribers using different information services;

6) improving the physical security of data stored on two-way systems (e.g. encryption, audit trails, double and triple passwords for access to sensitive data);

7) making the common carrier (whether cable or telephone companies) legally responsible for the confidentiality and security of information moving through its systems;

8) regulating third-party access to personal information derived from two-way services.[16]

Dr. Arthur Cordell, Science Council of Canada and Department of Communications

Dr. Arthur Cordell is a respected researcher who has published extensively on the social, economic and personal consequences of the increasingly widespread use of computers and information technologies. On the subject of privacy, he has outlined three concerns which he feels are likely have negative consequences for personal privacy in an information age.

1) An information infrastructure is being put in place very rapidly which will include details on all types of personal transactions, including legal, medical and educational activities. This electronic trail can be maintained cheaply and in perpetuity using computer technology.

2) With computer networks and increasingly standardized communications protocols, it will become feasible and inexpensive to interconnect many databases.

3) In Canada, there are no integrated set of laws to protect individual privacy.[17]

While he shares Professor Flaherty's apprehensions about the invasion of personal privacy, Dr. Cordell also suggests that

---

[16] Flaherty, pp. 143-149.

[17] Arthur J. Cordell, The Uneasy Eighties: The Transition to an Information Society. Background Study 53. Ottawa: Minister of Supply and Services, 1985, pp. 74-75.

individual conventions about privacy may be changing over time. He detects less concern among the public about confidentiality, as reflected in media talk shows where individuals seem prepared to reveal the most intimate details of their personal lives.[18] Whether this indicates a longer-term trend toward indifference about privacy invasions, or whether it is simply that privacy is a "public good", like the environment, that will not be defended until the situation becomes intolerable, is still open to speculation.

John W. Grace, Privacy Commissioner

Mr. John Grace has been Canada's Privacy Commissioner since the the Privacy Act came into force on July 1, 1983. He has been particularly articulate about the dangers of computer linkage as a threat to personal privacy (of which more will be said in Section 2 of this paper):

> ... covert computer linkage with unauthorized data matching is a form of search and seizure about which privacy advocates should be sounding alarms to both the government and the public. Such intrusions upon personal records should be subject to procedural safeguards at least as rigorous in their own way as those covering wire tapping to detect criminal activity or the search and seizure of property.[19]

Yet, while the dangers of data matching have not abated with time, there has been a noticeable backing away by the Privacy Commissioner from the problems this poses outside his area of jurisdiction (all federal government departments and a number of federal government agencies).

> The general principles enunciated in broadly-applied legislation may not well serve diverse groups. For example, it is highly doubtful that the Privacy Act, however ingeniously (or monstrously) elaborated, can be an effective code of fair information practice at the same time for, not only video stores, but the direct mail industry, credit bureaus and cable television.[20]

---

[18] Personal conversation with Dr. Cordell, January 11, 1989.

[19] John W. Grace, Annual Report, Privacy Commissioner, 1983-84. Ottawa: Minister of Supply and Services, 1984, p.4.

[20] John W. Grace, Annual Report, Privacy Commissioner, 1987-88. Ottawa: Minister of Supply and Services, 1988, p.7.

Such caution may be entirely understandable in an agency already overwhelmed by the volume of privacy violations it has to respond to within its current mandate, but it does little to reassure those who perceive a growing threat to privacy from data matching in the private sector.

International experts

Office of Technology Assessment, Congress of the United States

The Office of Technology Assessment (OTA) in the United States has taken an activist approach to the issue of privacy in electronic record systems, publishing several comprehensive and well-researched reports on the subject. Overall, it has concluded that:

> Federal agency use of new electronic technologies in processing personal information has eroded the protections of the Privacy Act of 1974. Many applications of electronic records being used by Federal agencies, e.g. computer profiling and front-end verification, are not explicitly covered either by the act or subsequent OMB guidelines. Moreover, the use of computerized databases, electronic record searches and matches, and computer networking is leading rapidly to the creation of a de facto national database containing personal information on most Americans. And use of the social security number as a de facto electronic national identifier facilitates the development of this database. Absent a forum in which the conflicts generated by new applications of information technology can be debated and resolved, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems.[21]

The OTA has identified a number of ways the U.S. federal government might respond to this situation, including:

1) doing nothing, which would represent an endorsement of the creation of a national database and a national identification number;

---

[21] Office of Technology Assessment, Federal Government Information Technology: Electronic Record Systems and Individual Privacy. Washington: U.S. Government Printing Office, June 1986, p. 99.

2) establishing control over federal computer-matching, front-end verification and computer profiling;

3) implementing more controls on sensitive personal information;

4) controlling and enforcing the security of personal information in a microcomputer environment;

5) legislating more specific guidelines for accuracy and completeness of records;

6) restricting the use of the social security number;

7) limiting inter-agency access to personal information;

8) strengthening existing institutional mechanisms for protecting privacy at the federal level or creating a new one (a data protection or privacy board);

9) undertaking a study of the broader social, economic and political context of information policy, of which privacy is a part.[22]

So far, the first option appears to be the action adopted.

James E. Katz, Bell Communications Research

Dr. James Katz's area of expertise is telecommunications privacy, and he has written extensively on the subject in a number of journals. He has made several predictions about possible privacy trends in the American telecommunications environment which are also relevant to the Canadian scene. They are that:

1) the expectation of privacy will continue to expand since it is positively correlated with increasing standards of living and is deeply entrenched in the American value system;

2) telecommunications and computer technologies will strengthen the value of privacy to people and sensitize them to its possible loss since more and more of people's personal life will be conducted over these media. This concern will likely stimulate new laws and regulations to protect privacy;

3) individuals will increasingly demand the right to

---

[22] Office of Technology Assessment, pp. 99-100.

review and correct data files held on them by organizations, and will likely be supported in this demand by the courts;

4) public opinion polls will show high and growing levels of concern about privacy invasion as information services become more commercialized, and governments can be expected to react to this public pressure, even if it means restricting the rational and efficient development of telecommunications services;

5) the rapid pace of telecommunications change will add to public disquiet about privacy invasion, since people tend to react negatively to the unfamiliar, especially if they perceive that they are losing control over a vital part of themselves to "exploitative machines";

6) as a countertrend, organizations will demand ever more privacy invasive information about individuals with whom they have contact as the demands for "hard data" on which to base decisions increases. Therefore, the information possessed by telephone service providers will become more valuable, both commercially and as a means of social control. The temptation to sell this data will become correspondingly greater.[23]

Dr. Katz also offers the interesting insight that a strong and diverse coalition of economic and civil liberty groups is the most effective means of gaining significant legislative protection for personal privacy. He notes that the Reagan administration's initial opposition to the 1986 Electronic Communications Privacy Act was largely eliminated once it was assured that organizations such as AT&T and the Videotex Industry Association supported the legislation as a means of overcoming customer misgivings about the security of communications on their networks.[24]

Justice Michael Kirby, New South Wales Court of Appeal

Justice Kirby, a former member of the Australian Law Reform Commission, was the Chairman of the Expert Group on Transborder Data Barriers, established by the Organization for Economic Cooperation and Development (OECD) in 1978 to

---

[23] James E. Katz, "Public policy origins of telecommunications privacy and the emerging issues", Information Age, volume 10, no. 3, (July 1988), pp. 173-176.

[24] Katz, "U.S. telecommunications privacy policy", Telecommunications Policy, (December 1988), p. 361.

draft the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. He has been credited with doing much of the work to develop the Guidelines[25] and is a respected voice in the international privacy community.

In a forum on access to information and privacy held in Ottawa in 1986, Justice Kirby propounded ten "information commandments" representing his assessment of the state of privacy protection in an information environment.

1) Contemporary technological developments endanger human rights and civil liberties and require responses from society -- including the legal system.

2) The fertile common law system, even as enhanced in some countries by constitutional rights, is insufficient to provide adequate responses to the challenges of technology. More legislation is needed.

3) In some cases, the technology itself demands or even produces legal reform because it renders current laws irrelevant or ineffective.

4) The people are not always the best judges of their own interests. Informed observers have a duty to identify dangers to freedom.

5) The costs of information rights must be counted; but so must the intangible benefits.

6) Information laws must be developed flexibly because of changing technology and the rapidly changing perceptions of the problem.

7) Information rights must extend from the public sector (where they have been developed) to the private sector. Voluntary guidelines, such a compliance with the OECD privacy principles, may provide a starting point but are likely to be inadequate in the longer term.

8) Information technology presents international issues that require international solutions.

9) Legal responses to information rights must attend to real problems and not content themselves with myths and mere symbols. (e.g. that information laws depending exclusively on individual motivation for enforcement will provide effective protection against abuses of new technologies).

---

[25] McDowell, p. 154.

10) Democratic values must be preserved, and it is at least questionable whether our democratic institutions can adequately respond to the challenges of technology. The tendency to parliamentary inaction is understandable, but dangerous.[26]

Justice Kirby believes that the ability of democratic institutions to cope with privacy and freedom of information in the face of rapidly changing technology will determine whether new information technologies become instruments of progress or inherently elitist and autocratic tools, perhaps in the end undermining democracy itself.

2. Specific privacy issues

The reader will have, by now, gained a general idea of the major privacy concerns of the public and experts. This section will focus on those issues that are of particular relevance in an advanced information services environment.

2.1 Privacy of content and privacy of process

It is useful to distinguish between the two types of privacy invasion that can take place in a communications environment.

Invasion of privacy content takes place when the substance of a message is intercepted, diverted, recorded or monitored by a third party. The most common current privacy invasion of this type is an illegal telephone wiretap.

Invasion of privacy process occurs when a third party makes use of records on who uses an electronic service, when it is used and what was the outcome. Examples of this kind of privacy invasion include monitoring of numbers dialled from a particular telephone or viewing patterns of pay-per-view cable subscribers. In this case, the substance of the message is of less interest than the pattern of consumption or usage revealed. As such, this information is of particular interest to marketing analysts and commercial firms.[27]

---

[26] Justice Michael Kirby, "New technology and international privacy issues", in Challenges and Change: Australia's Information Society. Ed. Trevor Barr. Melbourne: Oxford University Press in association with the Commission for the Future, 1987, pp. 150-158.

[27] Katz, "U.S. telecommunications privacy policy", p. 353.

2.2 Surveillance of content

Electronic eavesdropping in the form of wiretaps has chiefly been used in Canada by the police and security services for law enforcement or intelligence gathering purposes. There are a number of legal sanctions (particularly the Protection of Privacy Act) against the use of wiretapping devices for illegal purposes, and the security and intelligence files of the Privy Council Office, the Canadian Security Intelligence Service and the Solicitor General remain exempt from public access. Although these files are protected from unauthorized access to their contents, there are those who view such surveillance by the federal government with suspicion. A 1986 study done for the Law Reform Commission of Canada pointed out that electronic eavesdropping has been used by police forces in Canada much more frequently than originally intended by the Protection of Privacy Act. In fact, the relative number of wiretap authorizations in Canada is twenty times the number in the United States:

	U.S.	Canada
1975	701	1,123
1976	686	1,218
1977	626	1,304
1981	589	1,059 [28]

These "pre-Charter of Rights and Freedoms" statistics may reflect Canada's relative willingness, in contrast to the United States, to give greater weight to a societal value (security) than to an individual right (privacy) when justifying electronic intrusions. This tendency may, however, be modified by the legal impact of the Charter since 1982.

New information technologies have extended the potential for content surveillance or interception beyond the realm of voice communications on conventional wires to such areas as electronic mail and high speed data transmissions by microwave, satellite and optical fibre. Also falling into this category would be eavesdropping carried out using optical systems, microphones, pagers and video cameras, as well as cable TV and VDT (computer terminal) monitoring. Another issue of growing concern is workplace monitoring of telephone calls and electronic monitoring of the productivity of cashiers, airline personnel and telephone operators. All of these developments are posing challenges

---

[28] Law Reform Commission of Canada, Electronic Surveillance. Working Paper 47. Ottawa: Law Reform Commission of Canada, 1986, p. 10.

for lawmakers and regulators.

In the United States, the Electronic Communications Privacy Act, passed in 1986, protects nearly all forms of electronic communications, as well as the computer facilities involved in such communications. Stiff penalties have been specified if private interceptions are made for commercial gain, with lighter penalities levied in the case of casual intercepts. Interestingly enough, the radio portion of cordless telephone calls is exempted from the legislation: because of the ease with which such calls can be intercepted, the lawmakers wanted users to assume that conversations were not private.[29]

In Canada, the illegal interception of content in electronic form is covered by a number of statutes (which will be discussed in detail in Section 3 of the paper), so the situation is not nearly as neat as in the United States. The Privacy Commissioner in his 1985-86 Annual Report, points out that the natural "home" for legislative protection against attacks on privacy through electronic devices is the Protection of Privacy Act (which he does not administer). However, he goes on to say that:

> ... the present relationship between the Protection of Privacy Act and the Privacy Act is untidy and unsatisfactory. The division is based on distinctions which are hard to maintain because the old divisions have broken down.
>
> The use of computers to link information or to draw up personal profiles is no less electronic surveillance than listening to telephone conversations. The new technologies and the threat do not respect separate statutory compartments. It is at least an anomaly that someone called the Privacy Commissioner can speak out against one kind of breach of privacy but has no mandate to speak out against, much less prevent, breaches which are different only in method and may in fact be much more insidious.[30]

Although this situation has less applicability to information services that are sold on the telecommunications or cable systems with the express purpose of being

---

[29] Katz, "U.S. telecommunications privacy policy", pp. 357-8.

[30] John W. Grace, Annual Report, Privacy Commissioner, 1985-86. Ottawa: Minister of Supply and Services, 1986, p.10.

intercepted or monitored, the Privacy Commissioner's comments have particular relevance when it comes to the question of privacy of process or usage, which is addressed in the next section.

2.3 Surveillance of process or usage

David Flaherty, the Canadian privacy expert, has described in some detail the potential for accumulating transactional information on individuals or groups of individuals through the monitoring of interactive services. In his book, Protecting Privacy in Two-Way Electronic Services, he reviews a number of existing and proposed cable-TV applications, such as pay-per-view services, security services, public opinion polling, tele-education, tele-banking and tele-shopping, which require the storage and use (for billing purposes) of large amounts of information on the behaviour of subscribers. His list of potential privacy invasions through this technology include:

1) monitoring of TV viewing habits (both household and aggregate viewership);

2) continuous monitoring of movement in and out of a home;

3) storage and collection of data on subscriber opinions about issues on which he or she has been polled;

4) development of profiles on the buying habits of consumers;

5) development of profiles of the information retrieved by a subscriber from on-line databases;

6) criminal or unauthorized use of personal financial information stored on telebanking systems.[31]

The American privacy expert, Alan Westin, has suggested that at least four issues will have to be faced by those involved in telebanking and, eventually, by those offering any type of interactive service. First, how long should transactional data be stored? Westin believes that there will be enormous pressure from government regulators, marketers and researchers for access if data is kept for any length of time. Second, how secure is the data? Third, what protection will there be against creation of integrated profiles? Finally, how will third party access to the data

---

[31] Flaherty, pp. 44-80.

be controlled?[32]

In the United States, in the telecommunications field, considerable attention has been paid in recent years to such data, which are now referred to as Customer Proprietary Network Information (CPNI). The Federal Communications Commission has, in fact, issued regulations to govern the release of CPNI to firms that want to use them for marketing and planning purposes. Each multi-line business customer now has the right to decide which of the telecom information service vendors can have access to its CPNI. For example, records of numbers to which calls have been made are considered the property of the firm that made the calls and are not released except with the consent of the firm. Therefore, control of the data remains in the hands of the data generator, not the original service provider, the telephone company.[33]

An interesting loophole in these regulations has recently come to light, however. Major users in the United States, such as banks and insurance companies, have discovered that nothing appears to be preventing the carriers from passing telecom traffic statistics, for example, on to its own subsidiaries and marketing personnel. Members of the Telecommunications Association, a large users group, are appealing to the FCC to clarify the definition of CPNI and the rules of access to it.[34]

2.4 Data matching and linkage of personal information

Probably the most disturbing privacy violation that occurs in electronic environments is the matching of data from one source with data from other sources to produce profiles of individuals or groups. Through this technique, information which is fairly innocuous when stored in a discrete database becomes intrusive in the extreme when combined with information from other databases. For example, home telephone numbers on an electronic database could be matched with political party memberships or income information, then sold to canvassers or telemarketers, leading to a targetted

---

[32] Alan F. Westin, "Privacy Issues and the Implications of In-Home Banking," American Banker, June 3, 1981, quoted in Flaherty, p. 71.

[33] Katz, "U.S. telecommunications privacy policy", pp. 362-63.

[34] Kathy Chin Leong, "TCA pushes for privacy on corporate networks", Computerworld, October 3, 1988, p.133.

telephone solicitation campaign.[35]

The Canadian Privacy Commissioner has been sounding the alarm about this problem for many years. In 1981, the then Privacy Commissioner, Inger Hansen, advocated an amendment to the Criminal Code to create an offense against the "privacy of another". This enactment would have required "recipients or collectors or personal data to disclose to the person providing the data all proposed uses of the data not already explicitly provided for or made compulsory by law. The disclosure would be at the time of collection, and consent to new uses would be necessary". The law would have covered information given to governments, doctors, insurance brokers, banks and other institutions.[36]

This spirit of this recommendation has not been acted upon except at the federal level (see Section 4), but the Privacy Commissioner has continued to point out the dangers of the practice:

> Computer-matching turns the traditional presumption of innocence into a presumption of guilt. In matching, even if there is no indication of wrong-doing, individuals are subject to high technology search and seizure. Once the principle of matching is accepted, a social force of unyielding and pervasive magnitude is put in place.[37]

In January 1989, the Privacy Commissioner made a submission to the CRTC, expressing his concern about Bell Canada's plans to computerize its directory listings. He pointed out that a Toronto Company, Reteaco Inc. had matched computerized listings with Statistics Canada demographic data and Canada Post postal codes to produce profiles of 8.9 million households. Within each postal code unit of 100 to 1,000 people, Reteaco was able to determine levels of income, ethnic and religious composition of the households, the type of dwelling, marital status and numbers of children. Grace warned that, "it may be marketer's dream but it's a privacy nightmare". The president of Reteaco

---

[35] Example cited by Katz, "U.S. telecommunications privacy policy", p. 363.

[36] Inger Hansen, Report of the Privacy Commissioner on the Use of the Social Insurance Number. Ottawa: Privacy Commissioner and Department of Justice, 1981, p. 211-217.

[37] John W. Grace, Annual Report, Privacy Commissioner, 1985-86. Ottawa: Minister of Supply and Services, 1986, p. 7.

dismissed these concerns as "trying to shut the barn door after the horse has bolted", saying he only put together information that was already publicly available.[38]

How extensive is the practice of data matching and linkage? A special survey of 12 agencies done by the Treasury Board Secretariat in 1984-85 revealed that 53 separate matching programs were being carried out in the name of efficiency and prevention of fraud. For example, Revenue Canada cross-matches income tax and employment records routinely to ensure compliance with the Income Tax Act, while Employment and Immigration does similar data matching to detect unemployment insurance overpayments or fraud. The Canadian Security Intelligence Service can also, by obtaining warrants from the Federal Court, enter any public or private database, except for Statistics Canada's, either overtly or covertly.[39]

In the United States, an inquiry by the Office of Technology Assessment found that 43 per cent of the agencies surveyed (16 of 37) did computer matching. Eleven departments and four agencies carried out 110 matching programs, with a total of 553 matches carried out between 1980 and 1985. The total number of records matched was reported to be over 7 billion. Moreover, between 1980 and 1984, the number of computer matches done by the U.S. federal government nearly tripled.[40]

There is no way of knowing the extent of computer matching in the private sector because figures are simply not available.

A workshop sponsored by the Science Council of Canada in 1985 asked the following questions about computer matching:

1) Should covert computer linkage with unauthorized data matching be considered a form of search and seizure?

2) Should computer matching be covered by provisions of the Criminal Code, with provisions at least as comprehensive as those now required for authorized

---

[38] Iain Hunter, "Privacy dangers lurk in computerized lists, commissioner warns", The Ottawa Citizen, January 20, 1989, p. A-3.

[39] Science Council of Canada, A Workshop on Information Technologies and Personal Privacy in Canada. Ottawa: Minister of Supply and Services, 1985, pp. 26-27.

[40] Electronic Record Systems and Individual Privacy, p.38.

wiretapping?

3) Why should intrusions upon personal records, even in the name of efficiency and crime detection, not be subjected to procedural safeguards as vigorous as those covering wiretapping or the search and seizure of property?[41]

These questions have proved easier to answer in the public sphere than the private one. Preventing data abuses in the private sector runs the very real risk of impeding growth. As one participant at the Science Council workshop indicated, there is conflict between the principle of non-derivative use (not allowing information collected for one purpose to be used for another purpose) and the concept of information as wealth:

> If information is wealth, it is only wealth in the sense that companies can develop additional uses for it; and frequently those uses would be labelled as being non-derivative. I don't think policy makers in government or academics have yet addressed the question of how to balance information as wealth with the non-derivative use principle.[42]

Those aspects of the privacy problem that the policy makers have addressed are the subject of the next section of this paper.

3. Current state of privacy protection in Canada

In Canada today, as many experts have pointed out, there is no comprehensive, integrated set of legal rules respecting all aspects of the interest in privacy. However, there are protections in place which deal with various aspects of the subject. Whether these protections are adequate in an era of widespread information storage and processing on computerized systems is a topic that will be discussed in the final section of this paper. This section will simply describe the measures that are in place and give a brief assessment of their effectiveness.

3.1 Charter of Rights and Freedoms

Article 12 of the Universal Declaration of Human Rights, signed by Canada in 1948, states that "No one shall be subjected to arbitrary interference with his privacy,

---

[41] Science Council of Canada, p. 27.

[42] Science Council of Canada, p. 34.

family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

Canada's own Charter of Rights and Freedoms does not provide such explicit protection for privacy, although it has been suggested that section 8, "Everyone has the right to be secure against unreasonable search and seizure", could be used as the basis of limiting data linkage and unauthorized use of personal data on electronic information systems. This section of the Charter has, in fact, been tested in the courts in 1984 (Hunter vs. Southam Inc.) when the Supreme Court ruled that section 8 of the Charter, like the Fourth Amendment of the U.S. Constitution, protects the individual's reasonable expectation of privacy and requires a balance between an individual's privacy and the government's interest in law enforcement. This interpretation would be particularly applicable to electronic surveillance by the police, but it is not clear whether it would extend to electronic surveillance by anyone else.[43]

Dr. David Flaherty has suggested that one way of ensuring that protection is extended against all types of electronic intrusions would be to amend the Charter to create a basic constitutional right to privacy. Such a right was, in fact, proposed to the Joint Senate-House Committee on the Constitution by the Honourable David Crombie, but was defeated in 1981.[44]

3.2 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

On June 29, 1984, the Government of Canada announced that it was formally adhering to the Organization for Economic Cooperation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. As indicated earlier in this paper, the OECD had become concerned about this issue in the early 1970s and sought to protect privacy while at the same time ensuring that legislation in its member countries did not interfere unduly with world trade.

The Guidelines are a set of recommendations for minimum standards for the treatment of data, whether in manual or automated form. They consist of eight core principles, constituting a simple code of fair information practices:

---

[43] Law Reform Commission of Canada, pp. 8-9.

[44] Science Council of Canada, p. 48.

1) informed consent from data subjects 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) advance identification of the purposes for data collection;

4) restrictions on the re-use of data for new purposes without the consent of the data subject 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;

8) accountability of the data controller for compliance with data protection measures.[45]

Adherance to the Guidelines has certain implications. For the public sector, it means that member countries must:

1) adopt appropriate domestic legislation;

2) encourage and support self-regulation by the private sector;

3) provide for reasonable means for individuals to exercise their rights;

4) provide to adequate sanctions and remedies in case of failure to comply with the measures which implement the principles;

5) ensure that there is no unfair discrimination against

---

[45] Department of Justice, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Implications for Canada. Ottawa: Minister of Supply and Services, 1985, p. 5.

data subjects.[46]

For the private sector, endorsement of the Guidelines has two main implications -- they constitute the recommended principles upon which voluntary privacy codes should be based and they provide minimum standards that should be adopted to avoid interruption in the transfer of personal data between Canada and other member countries of the OECD.[47]

The remainder of this section deals with the public and private sector responses to the Guidelines.

3.3 The Privacy Act, July 1, 1983

Canada's original privacy protection statute was the Canadian Human Rights Act, proclaimed on March 1, 1978. Part IV of that Act outlined a code of fair information practices and established the post of Privacy Commissioner.

The most recent Privacy Act came into force on July 1, 1983. It provides individuals with access to any personal information held about them in government files, places limits on those who may see or use these data and gives individuals some control over the way the government collects and uses personal information. It also sets out a code of fair information practices, requiring the government to:

1) collect only the information needed to operate its programs;

2) collect the information directly from the individual concerned whenever possible;

3) tell the individual how it will be used;

4) keep the information long enough to ensure individual access;

5) take reasonable steps to ensure its accuracy and completeness.

Canadians may complain to the Privacy Commissioner if they are denied access to any personal information or if they are

---

[46] Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD, 1981, p. 12.

[47] Department of Justice, p. 3.

denied the right to correct information on their files. They also have recourse to the Privacy Commissioner if a department takes longer than 60 days to respond to their request, if the description of the government databank does not accurately reflect the uses that are being made of the information or if a department is collecting or disposing of information in a way which contravenes the Privacy Act.[48]

The Act applies to 145 federal government departments and agencies. Of the approximately 2,200 databanks held by these departments and agencies, only five are currently considered "exempt" from access by Canadians. Between July 1983 and December 1987, there were almost 160,000 requests by Canadians to see personal files. The Privacy Commissioner's office handled over 2200 complaints during that period about the lack of access, delays or misuse of information. Misuse of information and irregularities in the collection and disposal of data constituted about 8 per cent of the complaints caseload.[49]

An assessment of the first five years of the Privacy Act (albeit by the Privacy Commissioner, not an unbiassed observer) is that:

> Canada's Privacy Act continues to be applied with increasing sensitivity and rigor. While the application remains uneven, there can be growing, not shrinking, confidence that information which individuals give their federal government -- often with no choice -- will be used only for the purposes for which it is given and will be seen only be persons with the need or right to know.[50]

There are, however, those who believe that the Privacy Commissioner could be doing more to protect the privacy of Canadians in the light of advances in information technologies. This issue will be addressed in some detail in section 4 of this paper.

3.4 Protection of Privacy Act - June 30, 1974

The Protection of Privacy Act, as amended in 1977, enacted Part IV.1 of the Criminal Code making it an offence to

---

[48] Annual Report, Privacy Commissioner, 1987-88, p. 1.

[49] Annual Report, Privacy Commissioner, 1987-88, p.35 and p. 37.

[50] John W. Grace, Annual Report, Privacy Commissioner, 1987-88, p. 3.

intercept private communications, disclose private communications and possess equipment for the interception of private communications. To ensure that the police could still combat crime, provision was also made for judicial authorization of interceptions by law enforcement authorities.

"Private communication" within the scope of the Act means "any oral communication or any telecommunication made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it".[51]

The definition of "telecommunication" is the same one used under Section 287 of the Criminal Code which deals with theft of telecommunication service and possession of devices to obtain telecommunication services -- "any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system".[52] Despite the comprehensiveness of this definition, there remains some doubt as to whether it would cover the interception of communications transmitted over such devices as pagers and cordless phones.[53]

Since its enactment, the Protection of Privacy Act has been used mainly as a law enforcement device under which thousands of wiretaps have been authorized. There have been only a handful of prosecutions for unauthorized possession of interception devices by the general public, and these have been mainly for fairly unsophisticated equipment such as police scanners.

The Law Reform Commission has voiced some concern about whether the legislation does, in fact, protect privacy, since the number of wiretaps authorized under it have been about 20 times the per capita level in the United States. It has attempted, in a working paper on the subject, "to define the limits of lawful breach of the `right' to privacy.[54] It has also proposed that the definition of an "electromagnetic, acoustic, mechanical or other device" under the Act be amended to exclude "a pen register [a

---

[51] Criminal Code, s.178.1

[52] Interpretation Act, s. 28.

[53] Law Reform Commission of Canada, p. 19.

[54] Law Reform Commission of Canada, pp. 7-8.

device which records numbers dialed from a telephone], touch-tone decoder, diode device or other similar device sued to acquire the identity of the telephone number dialed, or of the caller, the time and the date of the telephone call, but which is not capable of intercepting any words or other information".[55] If this amendment is indeed accepted, it would appear to open the way for the type of usage monitoring that is causing concern among civil libertarians.

3.5 Criminal Code - Computer crime and data abuse

One of the primary privacy related concerns of the computer and data processing industries is the security of data on automated systems. According to The Economist:

> ... companies in France suffered at least 15,000 breaches of computer security in 1986. About 70% of them are thought to have been committed by the companies' own employees. A report earlier this year by Coopers & Lybrand, a firm of accountants, found that only one out of a sample of 20 large European companies was "adequately secure".[56]

In November 1988, a young hacker named Robert Morris released a virus into an American computer system that in only two days spread to 6,000 computers, widely cloning itself and causing the machines to fill their memories to a point at which they could not function.[57] According to the FBI:

> Prosecution under the Computer Fraud and Abuse Act will be difficult because its language is subject to different interpretations, has not been clarified in court and has not been used in a computer virus case before.[58]

In Canada, amendments to the Criminal Code, which received Royal Assent on December 5, 1985, have been introduced to deal with computer crime and data abuse of this nature.

---

[55] Law Reform Commission, p. 20.

[56] "Keeping out the Kaos Club", The Economist, July 9, 1988, p. 77.

[57] Michael Alexander, "Security, ethics under national scrutiny", Computerworld, November 14, 1988, p.6.

[58] Mitch Betts, "Virus' `benign' nature will make it difficult to prosecute", Computerworld, November 14, 1988, p. 16.

They are section 301.2 regarding unauthorized use of a computer and section 387.1(1.1), which introduces the concept of mischief in relation to data.

Section 301.2(1) states that:

> Everyone who, fraudulently and without color of right,
> a) obtains, directly or indirectly, any computer service,
> b) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or
> c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 387 in relation to data or a computer system,
> is guilty of an indictable offence an is liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Section 387.1(1.1) states that:

> Everyone commits mischief who willfully
> a) destroys or alters data;
> b) renders data meaningless, useless, or ineffective;
> c) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.[59]

An analysis of these provisions of the Criminal Code, done by Dr. Jake Knoppers for the Department of Communications, concludes that they will be effective in making illegal any form of eavesdropping or unauthorized access to a computer system, as well as deliberate alteration or deletion of data and theft of computer programs.[60] In other words, they will supplement the protection available under the Protection of

---

[59] Dr. Jake V.Th. Knoppers, Legal Issues Arising Out of Integrated Information Systems: An overview of Practical Considerations and Recent Developments. DOC-CWARC-87-E-CO4. Laval: Canadian Workplace Automation Research Centre, 1987, pp. 9-10.

[60] Knoppers, pp. 9-11.

Privacy Act against intrusions on content. It would appear, on the surface, that they will not prevent privacy intrusions on the usage of information services, as discussed earlier in this paper.

3.6 Other federal legislation and regulations

Other federal statutes placing limits on the disclosure of personal information include the Income Tax Act, chapter 3, section 241 and the Statistics Act, chapter 15, sections 6 and 16. As has become evident, however, nothing prevents commercial interests from using aggregated data from Statistics Canada databases, cross-matched with information from other sources, to develop profiles of consumers in neighbourhoods.

In 1986, the CRTC wrote privacy protection measures into its Terms of Service for federally regulated telephone companies. These regulations set out the rights and obligations of both the companies and their customers. Article 11 of the Terms of Service prevents disclosure of personal information regarding the customer, other than the customer's name, address and listed telephone number, without authorization in writing unless legally required. Exceptions to this rule are the customer him or herself, an agent of the customer, another telephone company (when required for the efficient and cost-effective provision of service), a company supplying telephone or telephone directory services or a collection agency.[61] While these terms give a considerable amount of protection to customers, the type of information that can be released, together with the exception for companies "supplying telephone or telephone directory services", still leaves room for commercial data matching and consumer profiling as described above.

In the cable TV field, the CRTC's major policy statement on privacy in non-programming and interactive services came in October 1983 when it urged the industry to adopt voluntary subscriber privacy codes. Among the measures recommended by the CRTC were:

1) informing subscribers of a system's relevant capabilities;

2) obtaining prior subscriber consent for the collection of data, other than that required for day-to-day operations;

---

[61] Bell Canada, Ottawa-Hull Directory. Ottawa: Tele-Direct Publications, 1988, p. 40.

3) providing subscribers with reasonable access to personal records;

4) ensuring the security of such records;

5) destroying records no longer needed; and

6) keeping individual subscriber data confidential.

As David Flaherty points out, a voluntary code leaves open the question of enforcement, since the CRTC has few options at its disposal at the moment, other than the withdrawal of licences.[62]

3.7 Provincial legislation

Only two provinces, Ontario and Quebec, currently have privacy legislation which provides strong data protection along the lines of the federal Privacy Act.

The Quebec legislation, "An Act respecting access to documents held by public bodies and the protection of personal information", came into force on July 1, 1984. The law includes most of the standard provisions for fair information practices and, in addition, breaks new ground with regard to data matching. Transfers of data between government agencies in Quebec are limited to information required for economic or industrial purposes and for income support and security. When agencies wish to exchange personal data, they must submit a written proposal to the Quebec Access to Information Commission for approval. The Commission will only approve data matching if:

- the data is necessary for the receiving agency to carry out its mandate;
- it is not feasible to collect the data directly from the person whom it concerns;
- the data subjects are fully informed that the data may be exchanged; and
- the confidentiality of the exchanged data is guaranteed.[63]

---

[62] CRTC, Public Notice: CRTC 1983-245. Cable Television Service Tiering and Universal Pay Television Service. Ottawa: CRTC, October 26, 1983, pp. 19-20, quoted in Flaherty, p.124.

[63] Science Council of Canada, p. 28-9.

The Ontario privacy legislation -- The Freedom of Information and Protection of Privacy Act -- was passed in 1987. Like the Quebec legislation it sets out rules for fair information practices under Ontario law and within Ontario jurisdiction, establishes an Information and Privacy Commissioner and gives the individual the right to correct any personal information about him or herself that is contained in government databanks.[64]

The Privacy Acts of the other provinces which have them (Manitoba, 1970, R.S.M., chapter P-125; Saskatchewan, R.S.S. 1978, chapter P-24 and British Columbia, R.S.B.C., 1979, chapter 336) correct a deficiency in the public law by making it a civil wrong to violate the privacy of another, but they are not the equivalent of the data protection laws of Canada, Quebec and Ontario. These laws provide the right of redress if there has been an invasion of privacy, even if no financial loss has resulted from the invasion.[65]

Recent case law seems to suggest that commercial violation of data privacy entitles the aggrieved party to compensation. In Computer Workshops v. Banner Capital Market Brokers, the legal question at issue was whether the defendent (Computer Workshops) had the right to even attempt to use confidential information resulting from its dealings with Banner. The court in this case defined confidential information as:

- something which is not public knowledge, but which may be based on or derived from information which is in the public domain;

- information that is communicated under circumstances in which an obligation of confidence arises; and

- information whose unauthorized use could result in injury to the aggrieved party.

The court ruled in favour of the plaintiff, Banner, and, as one commentator noted, "removed the last shred of doubt ... about the unauthorized use of confidential information, whether or not a contract or secrecy agreement has been

---

[64] Government of Ontario, Freedom of Information and Protection of Privacy Act, 1987. Statutes of Ontario, 1987, chapter 25 and Ontario Regulation 532/87. Toronto: Ministry of the Attorney General, August 1988.

[65] Cohen, p. 666, footnote 155.

signed".[66] The question arises as to whether this would apply to misuse of personal information as well as commercial information.

3.8 Industry self-regulation

As indicated in Section 3.6, the CRTC has been active over the past few years in encouraging the telephone and cable companies to adopt privacy protection codes. However, CRTC jurisdiction does not extend to other potential information providers on advanced communications systems, such as banks and retail outlets. Therefore, it will be necessary in this section to look beyond the potential carriers at the state of privacy self-regulation in other sectors.

The CRTC's Terms of Service for federally-regulated telephone companies provide a means by which voluntary data privacy and confidentiality practices can be overseen and enforced. Similar oversight powers appear to be lacking in other sectors which handle large amounts of personal information (except for provincial legislation regarding credit reporting companies).

In June 1984, the Canadian Cable Television Association (CCTA) adopted a cable industry subscriber policy for its 380 member companies. In this policy, the industry pledges to ~~to~~ secure subscriber data and restrict its use to only authorized employees, to retain data only for as long as necessary and to collect no individualized data on viewing habits unless the subscriber has been informed in advance. It also indicates that third parties providing service to subscribers on the cable system would be required to adhere to these privacy guidelines. The CCTA policy is silent on the question of releasing aggregated information or subscriber mailing lists.[67]

The prevailing attitude among cable companies is that government regulation of two-way cable services is not required because it would not be good business to misuse personal information. They also believe that no privacy problems currently exist and that privacy is not a pressing concern among subscribers.[68]

---

[66] Dan Merisch, "EDP and the Law", Canadian Datasystems, December 1988, p. 30.

[67] "The Canadian Cable Television Association Cable Subscriber Privacy Policy", reprinted in Flaherty, pp. 155-6.

[68] Flaherty, p. 13.

The Canadian Life Insurance Association has developed privacy guidelines, as have several major insurance companies such as Aetna Casualty Company of Canada, London Life and the Excelsior Life Insurance Company.[69]

In the banking industry, while there is a common law tradition of confidentiality, the Bank Act does not address the issue of customer information privacy. In 1987, when the Standing Committee on Justice and the Solicitor General reviewed the Access to Information and Privacy Act, only the Bank of Montreal had published a privacy code, although the Royal Bank of Canada was working on one at the time. The Canadian Bankers Association also indicated that it was in the process of developing a privacy code for all federally chartered banks.[70]

The development of electronic funds transfer systems, which are already evident in the widespread use of automated tellers machines, are expected eventually to all but eliminate paper-based financial transactions. With the possibility of utilizing automated financial records to develop a detailed profile of an individual's every financial transaction comes an enormous potential risk to privacy. The banks claim to have implemented many kinds of security mechanisms for their databases and telecommunications networks, but many privacy experts believe that more should be done, particularly with regard to giving the customer the right to see and challenge the information in their financial records.[71]

The Canadian Direct Marketing Association, whose members make extensive use of geodemographic techniques (targetting individual consumers for marketing campaigns through the use of demographic information from small geographic areas), also has a privacy code. It claims that anybody can, through one telephone call, have his or her name removed from all mailing lists used for solicitation in Canada. The Association gets between 2000 and 5000 complaints a year from consumers about its members. Despite this, the direct marketing industry strongly opposes the application of privacy laws or policies in its area of operation, claiming that they "would be detrimental to the economic progress of

---

[69] Flaherty, p. 134.

[70] Open and Shut: Enhancing the Right to Know and the Right of Privacy, p. 75.

[71] See particularly the discussion of this subject in the Science Council of Canada's A Workshop on Information Technologies and Personal Privacy in Canada, pp. 18-19.

Canada".[72]

Perhaps the most sweeping recommendations with regard to regulation of the private sector have come from the Standing Committee on Justice and the Solicitor General, to which this paper will now turn.

4. Recent Privacy Developments

Over the past year or two, there have been a number of developments on the privacy scene at the federal level that are relevant to the topic of this paper -- data protection in an information services environment. This section will highlight those elements of most concern to DOC and the information services industries.

4.1 Open and Shut: Enhancing the Right to Know and the Right to Privacy - Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act and the Privacy Act

In March 1987, the Standing Committee on Justice and Solicitor General tabled a report in fulfillment of a statutory requirement for a five-year review of the Access to Information and Privacy Acts. This report contained 108 recommendations on all aspects of the two Acts. The following are those which deal with computerized data and advanced information services.

4.1.1 Computer-matching programs

> The Standing Committee agreed with the Privacy Commissioner's position on the risks of computer matching and data linkage and recommended that Treasury Board issue guidelines requiring that government institutions give sixty days advance notice of intended matches in the Canada Gazette, describe all current matching activities in the annual Personal Information Index, report clearly under what authority they were doing the match, and register any new bank resulting from data matching. The Committee also recommended that the Privacy Act prohibit all but the most circumscribed data matches.[73]

---

[72] Science Council of Canada, p. 32.

[73] Standing Committee on Justice and Solicitor General, Open and Shut: Enhancing the Right to Know and the Right to Privacy. Ottawa: Queen's Printer for Canada, March 1987, p. 44 (Recommendations 5.6 and 5.7.)

4.1.2 Controlling Use of the Social Insurance Number

The Privacy Commissioner had told the Standing Committee that "uncontrolled and general use of the SIN establishes a de facto national identifier with all its ominous and de-humanizing implications".[74] The Committee responded by recommending that a new section of Privacy Act be drafted to limit the collection and use of the SIN to those activities explicitly authorized by federal legislation or, alternatively, that there be a statutory prohibition against the federal government, the provinces or the private sector denying services or goods to an individual who refuses to provide a SIN.[75]

4.1.3 Electronic surveillance

The Standing Committee was of the opinion that the Privacy Act should not remain solely a data protection statute and that the Privacy Commissioner should have responsibilities with regard to the electronic monitoring of individuals as covered by the Protection of Privacy Act on wiretapping. It therefore recommended that the definition of personal information be broadened to include all types of electronic surveillance. To this end, videotapes, urine specimens, photographs and tape recordings should be added to the definition. The Committee also recommended that the Privacy Commissioner be given the power to monitor developments and investigate complaints about electronic surveillance in federal and federally regulated workplaces.[76]

4.1.4 Commitment to the OECD Guidelines on the Protection of Privacy

The Standing Committee thought the federal government should be doing more to foster voluntary privacy codes in the private sector in

---

[74] Standing Committee on Justice and Solictor General, p. 45.

[75] Standing Committee on Justice and Solicitor General, p. 46, recommendations 5.9 and 5.10.

[76] Standing Committee on Justice and Solicitor General, p. 72, recommendations 7.1 and 7.2.

compliance with the OECD Guidelines. It recommended that the Departments of External Affairs and Justice prepare a report on private sector compliance within 18 months.[77]

4.1.5 Coverage of the federally-regulated private sector

Taking as its starting point the 1980 report of the Krever Commission in Ontario, which uncovered numerous breaches of the confidentiality of health records, the Standing Committee argued that "a comparable investigative Commission for the federally-regulated sector would reveal much more customer concern about their privacy, especially in the banking system, than is currently known to the general public".[78] It therefore recommended that the Privacy Act be extended to the federally-regulated private sector and that the Privacy Commissioner be empowered to review and approve implementation schemes developed by organizations in that sector.

The federally-regulated private sector includes about 25,000 corporations involved in banking, cable television, broadcasting, telephony, pipelines, and transportation.[79]

4.1.6 Impact of information technology on individual rights

The Committee stated its belief that research and monitoring should be undertaken to ensure that Canadians' rights are protected in the emergence of an information society. The technologies that particularly concerned it included:

- expert systems used on personal information databases

---

[77] Standing Committee on Justice and Solicitor General, p. 74, recommendation 7.4.

[78] Standing Committee on Justice and Solicitor General, p. 75.

[79] Standing Committee on Justice and Solicitor General, p. 77, recommendations 7.5 and 7.6.

- optical character recognition methods of computerizing manual records
- distributed data processing and ad hoc data communication
- two-way electronic services
- electronic mail
- telephone call-tracking devices
- office automation including mail answering systems
- use of electronic tags and bracelets on individuals
- machine-readable passports.

It therefore recommended that the Privacy Commissioner, in consultation with the Departments of Justice, Communications, and Supply and Services, the CRTC, Treasury Board and the Science Council of Canada, have the power to oversee the impact of information technology on personal privacy in the public sector and the federally-regulated private sector. The Committee also recommended that the Privacy Commissioner have the power to initiate studies in this area or to undertake studies at the request of the House of Commons.[80]

4.1.7 Oversight of microcomputers

Noting that "neither the Department of Communications nor any other government institution submitted any evidence to the Committee on the social impact of microcomputers", the Committee recommended that the Department of Justice, Treasury Board and other government institutions work with the Privacy Commissioner to develop new policies and practices to cope with the emerging data protection problem posed by

---

[80] Standing Committee on Justice and Solictor General, pp. 77-8, recommendations 7.7, 7.8 and 7.9.

personal information held in microcomputers.[81]

4.1.8 Regulation of transborder data flows

The Committee did not believe that privacy aspects of transborder data flows had received adequate attention, and recommended that the Departments of External Affairs and Justice conduct a review of the implications of transborder data flows for the personal privacy of Canadians within a year. The Department of Communications, the Privacy Commissioner, the CRTC, the Science Council, provincial agencies and private associations were to be consulted during the course of this study.[82]

4.2 Access and Privacy: The Steps Ahead - Federal government response to the Standing Committee

The government's response to the Standing Committee's Report was published in 1987. In some cases, it was fully in accord with the Committee's recommendations. In others, it was silent or manifested a reluctance to pursue the course of action proposed by the Committee, probably because of resource constraints.

4.2.1 Computer matching

This was one area where the government agreed to practically all the Committee's proposed actions. While it was of the opinion that Privacy Act currently provides sufficient authority to control data matching, the government indicated that it would issue explicit policy directives to departments and agencies on the subject. The policy would ensure that:

- all matches are in accordance with the collection, use, disclosure and retention provisions of the Privacy Act;
- the head of each department or agency certify that these requirements had been met;
- each institution assess the costs and benefits of computer matching programs before

---

[81] Standing Committee on Justice and Solicitor General, p. 79, recommendations 7.10 and 7.11.

[82] Standing Committee on Justice and Solicitor General, pp. 80-81, recommendation 7.12.

undertaking them;

- the Privacy Commissioner be notified 60 days before a matching program is used;

- explicit reference to computer matching be made in the annual Index to Personal Information.[83]

As of January 1989, the Treasury Board had developed a draft policy on data matching for inclusion in the Administrative Policy Manual, but had not yet formally announced it.

4.2.2 Control of the Social Insurance Number

The government also agreed with the Standing Committee's recommendations on the Social Insurance Number (SIN) and announced that it would introduce a policy limiting the use of SIN to those activities authorized by legislation. Any departments using the number without such authorization will be asked to justify their actions. Individuals will not be penalized for refusing to give their SIN to government institutions, except where required by law. A public education campaign will also be launched to indicate which uses of SIN are required by law or approved by the Treasury Board.

Once its own use of SIN is regulated, the government also indicated that it would pursue the application of similar controls throughout the rest of the public and private sectors. If these controls are not undertaken voluntarily, the government has not ruled out legislation, including amendments to the Criminal Code to make it a criminal offence to request the SIN unless required by law.[84]

As of January 1989, draft guidelines on the use of SIN had been prepared by Treasury Board, but had not yet been implemented.

4.2.3 Electronic surveillance

---

[83] Department of Justice, Access and Privacy: The Steps Ahead. Ottawa: Minister of Supply and Services, 1987, p. 8.

[84] Access and Privacy: The Steps Ahead, pp.6-7.

The government did not agree to extend the Privacy Act's terms to include electronic surveillance, stating that it "should concentrate on data protection matters and only regulate the collection, use and disclosure or information about individuals produced by such surveillance and tests". It also felt that misappropriation of personal information in computerized form was covered by the 1985 Criminal Code amendments on computer crime and mischief.[85] (See Section 3.5 of this paper.) However, it agreed to "monitor" the situation to determine whether further action is required.

4.2.4 Commitment to OECD Guidelines

The government indicated that it had created a task force, in cooperation with the provincial and territorial governments, to promote public and private sector self-regulation in accordance with the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. It did not say who was heading the task force.[86]

4.2.5 Coverage of the federally-regulated private sector

Protection under the Privacy Act was to be extended to Crown Corporations, although not to courts, administrative tribunals and organizations such as the CBC, which have exceptional needs in this area. The government was, however, silent on the need to extend coverage of the Privacy Act to include the federally-regulated private sector, as recommended by the Standing Committee.[87]

In adopting this cautious approach, the government may have been influenced by the Privacy Commissioner's own views as stated in his 1987-88 Annual Report:

> ... while the dangers are real, the heavy hand of regulation should only be imposed if the private sector does not voluntarily take

---

85 Access and Privacy: The Steps Ahead, pp. 3-4.

86 Access and Privacy: The Steps Ahead, p. 12.

87 Access and Privacy: The Steps Ahead, p. 13.

steps to address them.[88]

He then goes on to speak approvingly of the CRTC's work on the telephone companies' Terms of Service, indicating that "a sectoral approach is being increasingly advocated and practiced".

As of January 1989, the legislative amendments extending Privacy Act coverage to Crown corporations had not yet been tabled.

4.2.6 Impact of information technology on human rights

The government was also silent on the Standing Committee's recommendation that more research be undertaken in this area, except to note the existence of the Science Council's 1985 study, The Uneasy Eighties: The Transition to an Information Society.[89]

4.2.7 Oversight of microcomputers

Within the government, it was agreed that there should be common management principles for information, regardless of the form in which it appears -- paper, microfiche, computer disks or tape or optical disk. Treasury Board has approved a policy in this area establishes consistent practices for the collection, disclosure, use, retention, disposal and security of information in conformance with the legal requirements of the Privacy Act.[90] This policy is interesting because it represents a tacit recognition by the federal government that "information" as an entity can no longer be tied to specific media but must be managed as a commodity in its own right.

4.2.8 Transborder data flows

The government agreed with the Standing Committee that the issue of privacy and transborder data flows requires study and indicated that it had "already begun to explore the means by which to

---

88 Privacy Commissioner, Annual Report, 1987-88, p. 7.

89 Access and Privacy: The Steps Ahead, p. 3.

90 Access and Privacy: The Steps Ahead, pp. 9-10.

determine whether such a problem exists".[91] It did not indicate through what mechanism this was taking place.

5. Conclusions and options

A great deal of ground has been covered in this paper, and it would probably be useful to review what has been said about information technologies, information services and privacy and to draw some conclusions before discussing the options that DOC might wish to pursue in this area.

5.1 State of privacy protection in Canada

Polling data, while incomplete and not entirely comparable from year to year, nevertheless indicates a growing public concern about the threat to privacy posed by automated information services. This uneasiness is echoed by leading experts on the subject who are particularly concerned about the potential for privacy violation through computer matching and data linkage and unauthorized third party access to personal data.

In Canada today, strong statutory protection against privacy invasion of the content of automated information services appears to exist through the provisions of the Protection of Privacy Act and the 1985 revisions to the Criminal Code. Similarly, the privacy statutes of Canada, Quebec and Ontario appear to provide redress against unauthorized intrusions upon the privacy of content and usage of automated information services managed by their governments. The situation is less reassuring in the other provincial governments where statutes on fair information practices do not exist.

It is in the private sector where the potential for major privacy problems appears the greatest, particularly in the area of data usage. As one computer trade journal noted:

> ... there is no protection today against "information vendors" releasing your most personal data - as long as they get the facts right. Libel and slander protect against damaging inaccuracy, but if an organization releases your social insurance number, your credit card numbers, your bank balance and your medical history, you have no

---

[91] Access and Privacy: The Steps Ahead, p. 13.

comeback.[92]

Voluntary self-regulation by the private sector is the option most often suggested to deal with this problem. As the Privacy Commissioner has himself suggested, "scrupulous compliance with the data protection principles set forth in the guidelines of OECD would be a good place to start". However, he has also observed that the Minister of External Affairs' appeal to the private sector to do so has produced no discernable impact so far.[93]

The usual reasons given for a "hands off" approach by government are the potential for interfering with commerce and the lack of any evidence of widespread data abuse in the private sector. Counterarguments by certain experts and investigative bodies suggest that privacy protection measures are not costly or difficult to manage and that the lack of evidence of widespread abuse is primarily the result of a lack of research.

Since DOC's current policy to encourage the widespread development and proliferation of interactive information services, whether via the telephone or cable networks or on media such as optical disks, it will be creating a situation where privacy problems due to data abuse could become much more serious. It is therefore desirable that the Department take into account the potential privacy threats of advanced information services when formulating strategies designed to accelerate their development. This is particularly critical since the major players in the information services industry will almost certainly be the telephone carriers, the cable companies, the software developers and the database vendors, all of which fall primarily or partially within the Department's sphere of operations.

Assuming that there will be growing pressure on information service providers to collect, manipulate and sell personal information acquired in the course of their business, what would be the minimum requirements for privacy protection of consumers in such an environment? The following is suggested as a minimum:

1) There be no personal data record-keeping systems whose very existence is secret.

2) There must be a way for individuals to find out what

---

[92] "A little disk may pose a huge threat", Computing Canada, March 19, 1987, p. 10.

[93] Annual Report, Privacy Commissioner, 1987-88, p. 8.

information about them is in a record and how it is used.

3) There must be a way for individuals to prevent information about them, which was obtained for one purpose, from being used or made available for other purposes without their consent.

4) There must be a way for individuals to correct or amend a record of identifiable information about themselves.

5) Any organization creating, maintaining, using or disseminating records of identifiable personal data must ensure the reliability of the data for its intended use and must take precautions to prevent misuse of the data.[94]

The next section will discuss the pros and cons of the various options that have been suggested for achieving these protections.

5.2 Options for action

5.2.1 Option 1 - self-regulation

Self-regulation is, naturally enough, the option that holds the most appeal for the private sector and that would be easiest for government to implement, since the only governing instrument required for its adoption is moral suasion. However, to be effective it requires a strong commitment from the companies delivering information services, as well as a mechanism whereby the consumer can gain redress if privacy violations are discovered.

One possible means of putting some clout into self-regulation is to require that firms providing information services incorporate the principles of the OECD Guidelines into their contracts with customers. This would have the effect of creating actionable rights for consumers. As the participants at the Science Council's workshop on information technologies and privacy concluded:

> In the absence of such actionable rights, customers of organizations are left with just a piece of paper -- a nicely worded privacy code --

---

[94] These basic principles were developed by the participants at the Science Council of Canada Workshop on Information Technologies and Personal Privacy in Canada, p. 33.

> that makes certain promises abut protecting personal privacy. In other words, voluntary guidelines or codes may look very good on paper, but in terms of giving people enforceable rights to privacy, they may be meaningless when they are not written into customer agreement contracts.[95]

Another means is to generate public pressure from those customers which would make it in the best interests for information service providers to adhere to privacy codes. The polling data seem to suggest that public sentiment is moving in the direction of greater privacy protection in electronic environments. However, it is a movement which has not as yet developed a public spokesman or advocate.

Self-regulation has also been justified as appropriate in the absence of any discernable problem. There is no ready answer to this argument because evidence simply does not exist outside of the public sector. As David Flaherty has pointed out:

> In Canada, we need empirical studies of the functioning of data protection on a sector-by-sector basis along the lines of what my mentor Alan Westin has done in the United States with health records, personnel records, and various other types of public- and private-sector data banks. We need to find out what is actually happening to personal information in some of these private-sector areas.[96]

If problems are discerned as a result of such investigations, there can be no doubt that they will increase exponentially as more and more data is stored in electronic form and made accessible for manipulation by second and third parties. As one privacy expert has noted, "a longer term problem will ... prove extremely challenging for the telephone companies, namely the treatment of data possessed by them. They will be continuously evaluating the possibilities of packaging and selling their data, especially as BISDN or other intelligent networks are implemented".[97]

Finally, there is the question of cost. The private

---

[95] Science Council of Canada, p. 44.

[96] Science Council of Canada, p. 48.

[97] Katz, "U.S. telecommunications policy", p. 366.

sector position has been that greater data protection will hinder the flow of commerce and impose enormous extra costs on them. This has been disputed by the Standing Committee on Justice and Solicitor General which, in its report suggested that "the burden and costs of extending such a stream-lined system of data protection to the federally-regulated private sector appear to be manageable and commensurate with the interests of Canadians that merit protection."[98] Again, no one is really sure. As the private sector begins to seek the maximum commercial value from the information stored on their systems, it could be that the opportunity costs of implementing adequate privacy protection could far exceed the actual costs.

5.2.2 Option 2 - Sector-specific regulation

A second option for the DOC to consider in the information services area is the introduction of specific regulations to ensure privacy protection, both of commercial and personal data.

The chief advantage of this approach is that the Minister of Communications, through the mechanism of the CRTC, has the mandate to set policy in at least two of the sectors that are likely to play a role in the delivery of advanced information services -- telecommunications and cable. As David Flaherty has noted:

> With respect to non-programming services, the CRTC has already built a case for the exercise of jurisdiction ... Thus, there seems to be no reason for the CRTC to adopt a minimalist position on data protection. If it develops a continuing will to act, few serious legal impediments exist to challenge its jurisdiction and those that do exist can be clarified by changes in the relevant federal statutes, if necessary. Since the federal Privacy Act of 1982 only regulates federal government data banks, it is also appropriate for the CRTC to deal with emerging privacy problems in the industries it regulates.[99]

The major impediment is that most, if not all, information services providers are likely to be Type II

---

[98] Standing Committee on Justice and Solicitor General, pp. 76-7.

[99] David H. Flaherty, p. 123.

carriers under the existing Telecommunications Policy and will therefore not be subject to regulation by the CRTC. An additional problem may arise in the context of the Free Trade Agreement with the United States, which might interpret Canadian attempts to limit third party access to personal data derived from the operation of information systems as an undue restriction of trade. On the other hand, if such provisions were to be applied across the board to all information services providers, regardless of national origin, and in accordance with the OECD Guidelines, they might be justified on the grounds of protection of human rights and of "harmonization" with privacy protection measures in other countries.

The Privacy Commissioner is on record as favouring a "sectoral" approach to data protection in the federally-regulated sector. The difficulty with information services is that the "sector" is likely to expand to encompass all manner of businesses, carrying out a variety of activities of which "information services" may be a vital component or a lucrative by-product. If one accepts the American position, articulated by the FCC, that Customer Proprietary Network Information (CPNI) is the property of the service provider, CRTC regulation of the carrier (i.e. the telephone or cable company) may prove to be an ineffectual means of protecting privacy since most of the data of concern will fall outside its area of jurisdiction.

5.2.3 Option 3 - Omnibus legislation

The regulatory equivalent of cutting the Gordian knot would be to create, through legislation, a new class of regulated sector called information services, which would be the equivalent of or successor to current acts governing the broadcasting and telecommunications fields. This would entail a number of jurisdictional, not to mention commercial, problems of implementation since, as noted above, it would encompass a broad spectrum of businesses for which information services might only be an incidental activity. Nevertheless, this approach would have the virtue of simplicity, inasmuch as it would provide consumers with similar privacy protection measures vis-a-vis all types of information services on all types of information technologies, at least in the federally-regulated sector.

Another option, which has been suggested (as noted above) by the Standing Committee on Justice and

Solicitor General, is to extend the jurisdiction of the Privacy Act to the federally-regulated sector. Under this legislative scheme:

> The Privacy Act would thus establish general rules for fair information practices for the federally-regulated private sector, and the Office of the Privacy Commissioner would oversee compliance, inlcuding the investigation of complaints that were not settled internally adn the protection of individual rights of access to data. Each organization subject to the new part of the Privacy Act would be required to establish the purposes and uses of the personal data it collects and to designate a senior person to be responsible for data protection within the corporation.[100]

The Privacy Commissioner himself has expressed some reservations about this recommendation, particularly with regard to the applicability of a broadly stated privacy code to businesses as diverse as direct marketers, cable companies and video stores. He has also appeared to be overwhelmed by the size of the task that would be involved. As mentioned earlier, the federally-regulated private sector includes some 25,000 firms. Even if the Act were applicable to firms with more than 500 employees, he estimates that it would require a three to four-fold increase in the human and financial resources of the Office of the Privacy Commissioner to fulfill his obligations.[101]

The advantages of this approach, as for the information services act option, is that it is simple, direct, avoids the proliferation of statutes and would not be limited to one type of technology. It also gives uniform protection to consumers of all information services within the federal and federally-regulated private sector, avoiding a "patchwork" of coverages and differing privacy rules.

5.3 Recommended DOC actions

The three options outlined in sub-section 5.2 of this paper need to be considered in greater depth before any decision is taken on DOC action with regard to privacy protection in information services. More groundwork needs to be laid to

---

[100] Standing Committee on Justice and Solicitor General, p. 76.

[101] Annual Report, Privacy Commissioner, 1987-88, p. 8.

determine the extent of action warranted. This sub-section will merely enumerate those that emerge most clearly from the analysis.

1) Polling data seem to suggest a growing concern among the Canadian public about potential invasions of privacy in electronic information services. However, the information currently available to the Department is uneven, incomplete or statistically limited in scope. DOC should therefore consider carrying out a comprehensive survey on privacy issues, possibly replicating the 1983 London survey on privacy and two-way cable television but using a larger, Canada-wide sample and readjusting the questions to focus on information services from a technology-neutral viewpoint. The results of such a survey will be useful for policy makers, not only in DOC, in determining whether Canadians' concern about the privacy issue warrants greater attention.

2) At the root of the current debate about extending data privacy protection beyond the public sector lies a fundamental lack of information about the extent of privacy invasions in the private sector. Only more research, along the lines proposed by David Flaherty, will answer that question. As pointed out earlier in this paper, the 1980 Krever Commission in Ontario uncovered extensive misuse of medical records which had been totally unknown to either the public or policy makers before the investigation took place. DOC should spearhead further research at the federal level to ensure that any choice of the options outlined above is based on empirical knowledge, rather than on speculation, inertia or political pressure.

3) DOC has had limited involvement in the privacy debate over the past decade or so. However, as Canada stands on the threshhold of an explosion of electronic information services in the coming decade, it is critical that the Department reassert its presence in this area.

   Personal conversations with the Privacy Commissioner and members of his staff indicated that they would welcome greater input from DOC on the broader issues being dealt with in the DGSP information services paper, particularly as the privacy of Canadians' personal, financial, medical and consumption data may be affected by the growing use of interactive, transactional technologies.

   In view of the role of the Departments of Justice and

External Affairs in encouraging private sector adherence to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, DOC should also consult them to determine how seriously the private sector is taking the data protection initiatives that already exist.

Finally, the extent of the CRTC's regulatory role in this area needs to be clarified. While it can regulate such matters as the selling of automated directory information, it has no mandate (and may desire no mandate) to oversee the privacy aspects of "downstream" applications of that information by service providers. Assuming that the Minister of Communications obtains the "power of direction" over broad CRTC policies, the CRTC's position may be more or less negotiable. Nevertheless, given the attention the Commission has devoted to interactive cable services over the past 10 years, its views on the privacy issue would be valuable input to DOC in the development of its information services policy.