PRIVACY & TECHNOLOGY: A CANADIAN PERSPECTIVE

MURRAY RANKIN*

After introducing the topic, the author proceeds to a discussion in which he considers the definition and value that various commentators have associated with the concept of privacy. He then goes on to examine the issue of privacy, specifically as it relates to computers and computer "data bases". The final section of the paper reviews and assesses the Canadian legislative response.

I. INTRODUCTION

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions . . . There are thus hundreds of little threads radiating from every man, millions of threads in all . . . They are not visible, they are not material, but every man is constantly aware of their existence.[1]

As long ago as 1964 the noted French sociologist, Jacques Ellul, decried the blind devotion of Western societies to what he termed "la technique".[2] In his theory, "la technique" represents the integration of the machine into society leading to a standardization and rationalization of economic and administrative life. Technical progress, he said, was irreversible in a given society and tended to act according to a geometric progression. Inherently dehumanizing, the internal laws of la technique binds individuals into a society "coordinating and systematizing their work; . . . [it] reigns alone, a blind force and more clear-sighted that the best human intelligence".[3] Ellul summarizes the motivating force for technical evolution by reference to the development of the atomic bomb: "Since it was possible, it was necessary." Everything in the modern society is increasingly focused solely upon the central principle of la technique: efficient ordering, the inherent dynamic of the machine.

On the other hand, the pessimism of social commentators like Ellul has been counterbalanced by the unbridled optimism of other observers of our times. Alvin Toffler and others argue that technology has allowed the individual a greater range of choice than has ever been enjoyed before. If technology poses certain problems, they can be solved by the application of more technology — the so-called "technological fix" will avail. If one accepts that technology is not going to disappear, then social policies should be directed toward the protection of humanistic values.

Canada like other post-industrial societies is caught in a "technological nightmare of opportunity" as a recent Minister of Communications has termed it.[4] It is estimated that practically one-half of Canada's gross national product and more than half of the employment of its citizens is related to the production, processing, storage and use of information [5] Accordingly, twin challenges face Canadian society in respect of in-

---

* Of the Faculty of Law, University of Victoria.

1. Alexander Solzhenitsyn, *Cancer Ward* (1968).
2. Jacques Ellul, *The Technological Society* (1964).
3. *Id.* at 93, 94.
4. Hon. David Macdonald cited in H. Janisch and M. Irwin, "Information Technology and Public Policy: Regulatory Implications for Canada" (1982) 20 *Osg. H.L.J.* 610, at 622.
5. R. Grant Hammond, "Quantum Physics, Econometric Models and Property Rights to Information" (1981) 27 *McGill L.J.* 47 at 48.

formation. Can new legal, economic and social arrangements ensure the creation and effective utilization of the new information technology? Can a liberal society protect its basic political and human values from unwise applications or restrictions of that new knowledge?[6] To some, the computer is merely a neutral machine; to others, it represents the "infrastructure of tyranny" and the embodiment of all that Ellul castigates in "la technique". McLuhan described the converging information transfer networks as society's electronic equivalent to the biological central nervous system.[7] Our culture has progressed from an agricultural to an industrial and now to a post-industrial society. Just as the success of pre-industrial societies was achieved by the proper management of energy and production processes, post-industrial societies are increasingly and inexorably based upon information management.

One of the many social issues which must be faced as the "information society" develops is the issue of privacy. To what extent is individual privacy threatened by this burgeoning computer technology? The parabolic microphone, the telescopic lens and infra-red photography are all examples of modern technological development which can be said to invade an individual's privacy. "Pen registers" are snooping devices which, when attached to a telephone line, are able to record the numbers dialed from a particular telephone. If information acquired by the pen register were automatically fed into a central computer for analysis, one's personal network of acquaintances could readily be determined.[8] The emerging optical scanner technology has produced a mechanical page reader capable of scanning and recording hundreds of pages of text per hour. Wiretaps installed on telephone lines and bugs implanted in rooms represent other, more commonplace methods of invading privacy in our modern society. The technology of Electronic Fund Transfer Systems may have a serious impact on one's privacy.[9]

This paper will not attempt to address the entire question of the technology available to modern government for the surveillance of its citizens. Instead, data protection laws as one governmental response to one manifestation of "la technique" will be considered. The analysis will examine these laws solely in the context of public sector information banks. It will focus particularly upon the Canadian experience with data protection legislation, initially contained in Part IV of the Canadian Human Rights Act.[10] This legislation was superseded by the Privacy Act[11] proclaimed as law on July 1, 1983.

First, the various definitions of the term "privacy" will be considered in order to situate the issue of data protection in some theoretical framework. How accurate is the apparent public perception that computers constitute a serious threat to individual privacy? Next, the specific

6. *See* speech of Mr. Al MacBain (Parliamentary Secretary to Minister of Justice and Attorney-General of Canada) in Parl. Deb. H.C., February 9, 1983 at p. 22678.

7. M. McLuhan, *Understanding Media: The Extensions of Man* (1964) at p. 304.

8. *See* Arthur R. Miller, *The Assault on Privacy*, (1971) at p. 43.

9. *See* R. McLaren, *Canadian Payments System* (Toronto: Ontario Electronic Funds Transfer Study Project, 1977).

10. S.C. 1976-77, c. 33.

11. S.C. 1980-81-82, c. 111. Royal assent was given on July 7, 1982.

privacy concerns raised by computer technology will be canvassed, with an evaluation of the costs and benefits of various policies suggested for the regulation of computers. The Canadian legal response to the problem of privacy protection in the age of computers will then be analyzed, culminating with a consideration of the recently enacted Privacy Act.

II. "PRIVACY": TOWARD A WORKING DEFINITION FOR AN INFORMATION SOCIETY

> Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is to be communicated to others.[12]

So begins the excellent Report of the Ontario Commission on Freedom of Information and Individual Privacy.[13] The concept of privacy has proven to be very elusive and is rarely adequately defined in the burgeoning literature in this field. Perhaps privacy is like obscenity in the eyes of the Justice Potter Stewart who could not define it but knew it when he saw it.[14] The most familiar, albeit conclusory definition of privacy, was provided by U.S. Judge Cooley who defined it simply as "the right to be let alone".[15]

In his seminal article on privacy, Dean Prosser took a functional approach. Analyzing some four hundred cases he concluded that "the right to privacy" in American law is a catch-all term directed at four distinct kinds of invasion of four separate interests: intrusions upon the plaintiff's physical seclusion or solitude, public disclosure of private facts, publicity which places the plaintiff in a false light and appropriation for the defendant's benefit of the plaintiff's name or likeness.[16] Alan Westin has suggested two additions to Prosser's list as a result of modern technology: psychological surveillance and data surveillance.[17] Like Prosser, Raymond Wacks, has provided at least seven examples in English law where the notion of "privacy" has become confused with other legal issues and urges that attempts "to insinuate" privacy into English law should be resisted.[18]

The status of privacy has been variously described as a situation, a right, a claim, a form of control and a value.[19] Privacy has been said to relate to information concerning the individual: his autonomy, personal identity and physical integrity. A Canadian Task Force on Privacy and Computers has identified three different contexts in which to analyze claims of invasion of privacy: (a) territorial privacy; (b) privacy of the person; and (c) privacy in the information context.[20] This third category,

---

12. Alan F. Westin, *Privacy and Freedom* (1967) at p. 7.
13. Vol. 3, *Protection of Privacy* (1980). ["Ontario Commission"].
14. *Jacobellis* v. *Ohio* 367 U.S 184 (1964).
15. Cooley, *Torts* (2nd ed., 1895) at p. 188.
16. William L. Prosser, "Privacy" (1960), 48 *Cal. L. Rev.* 383.
17. *Supra* n. 12, ch. 6.
18. R. Wacks, "The Poverty of 'Privacy' " (1980) 96 L.Q.R. 73.
19. *See* Ruth Gavison, "Privacy and the Limits of Law" (1980), 89 Yale L.J. 421 at 424.
20. Canada, Department of Communications and Department of Justice, *Privacy and Computers*, (Ottawa: Information Canada, 1972) at 13 - 14.

of particular significance in the present analysis, is said to be based primarily on the notion of the dignity and integrity of the individual.

The claim of informational privacy assumes that all information about an individual is fundamentally the property of that individual; for him to communicate or withhold as he determines. Sometimes the disclosure of confidential information might harm the individually financially or cause great embarrassment, even if the information disclosed is accurate. The context is, of course, the controlling factor in determining whether or not information will be damaging. Certain competing social values may necessitate disclosing personal information for particular purposes, for example census information. The individual may decide to disclose information in order to gain certain benefits such as credit information or information disclosed to a solicitor in order to win a lawsuit. Nevertheless, the individual has a continuing interest in controlling access to personal information. The Ontario Commission on Freedom of Information and Individual Privacy endorses Professor S.I. Benn's appealing definition that the state of privacy is simply that of "not sharing an experience, a place or knowledge with anyone else" or, where two or more people are enjoying a state of privacy together "there is sharing only because the subject wants to share".[21]

Professor Parker has considered as an invasion of privacy the aggregation of personal information by institutions which gather facts and opinions, not all of which would have been willingly disclosed by an individual.[22] He stresses, however, that what appears to be a loss of privacy in this context is in fact a loss of the *value* of privacy for the individual concerned. When information is gathered, one's "privacy" loses value because one of the main uses made of "privacy" is to control the flow of information about one's self. The gathering of information reduces the value of "privacy" by making it less secure. In addition, one's "privacy" is devalued by rendering it less secure as the individual is never certain whether it is still intact.

To some critics, such notions of privacy constitute merely bourgeois preferences — a value mainly of the middle class and upper-middle class.[23] Similarly, it has been asserted that this notion of informational privacy should be limited strictly to technically advanced Western cultures. However, there is considerable evidence that the need for personal privacy is a universal, common element of the human experience. It was evident in the customs and communal life of primitive tribes and was a factor in the social conditions of ancient Greece.[24] In the Western democracies, the assertion of a right to privacy was born out of the Enlightenment suspicion to the state. To paraphrase John Locke, the state was established to serve society, a group of individuals who lead their own private lives. Professor Westin links privacy with personal

21. Ontario Commission, *supra* n. 13, at 506 citing S.I. Benn, "The Protection and Limitations of Privacy" (1978), 52 Australian L.J. 601 at 602.

22. R.B. Parker, "A Definition of Privacy" (1974), 27 *Rutgers L. Rev.* 275.

23. *See e.g.*, A.S. Miller, "Privacy in the Modern Corporate State" (1973), 25 *Admin. L. Rev.* 231 at 232.

24. *See e.g.*, I.C. Velecky, "The Concept of Privacy" in J.B. Young, (ed.), *Privacy* (1978) at pp. 15 - 17.

autonomy or freedom, identifying the concern to preserve individual freedom as a major justification for the recognition of a right to privacy. If privacy is invaded, two aspects of personal autonomy are threatened: our relationships with other individuals and our relationships with institutions.[25]

Charles Fried contends that the concept of privacy as the control over personal information is a central element of personal liberty, an essential prerequisite to many "significant ends in life" such as "love, trust, friendship, respect, and self-respect".[26] Friendship and love cannot survive without privacy. An atmosphere promoting creativity is impossible without the trust founded on privacy. The important psychological utility of privacy is developed by Erving Goffman's writing on such "total institutions" as prisons and mental institutions.[27] Goffman's thesis is that the individual's integrity, development and preservation of personal identity requires the protection of a zone of privacy within which the ultimate secrets of one's "core" self are not involuntarily invaded. To the extent that modern technology can create an "information prison," freedom as we know it is threatened. Privacy without freedom may sometimes exist, as those in solitary confinement are aware, but there can be no freedom without privacy.

If individuals are treated as objects or as means to others' ends, privacy concerns are magnified. Widespread use of computer technology may promote a tendency to consult records as a substitute for face-to-face contact. Most record-keeping organizations consult the records of other organizations to verify information they obtain from an individual. They pay far more attention to what other organizations report than they pay to what the individual reports about himself. As the quality and quantity of personal information on computers increases, decision-makers may seek to avoid individual contact as much as possible resulting in the kind of dehumanization predicted by Ellul. The autonomous laws of "la technique", he argues, lead inevitably to an impersonal society in which individuals must sacrifice to the organization such cherished values as their privacy.

Since the notion of privacy has been so notoriously difficult to capture in a meaningful definition, Professor Freund suggests that the right to privacy should be regarded as "a principle having a high order of generality rather than a rule which will govern specific cases".[28] Although a spirited argument may be made to demonstrate that privacy is a neutral concept useful in legal contexts to identify occasions calling for legal protection, this conceptual thicket will not be entered for present purposes.[29] Instead, the notion of privacy in this paper will be that of Professors Westin and Miller who have focussed as "the individual's ability to control the circulation of information relating to him".[30]

---

25. *Supra* n. 12, at 33 - 34.
26. C. Fried, *An Anatomy of Values: Problems of Personal and Social Choice* (1970) at 140.
27. *Asylums: Essays on the Social Situation of Mental Patients and Other Inmates* (1968).
28. P. Freund, "Privacy: One Concept or Many" (1971), 13 *Nomos* 182 at 197.
29. *See* Gavison, *supra* n. 19 at 422.
30. *See supra* n. 12 and Arthur R. Miller *supra* n. 8, at 25.

Several writers do not champion informational privacy to the same degree as Fried, Westin and Miller. Fried's view of a right to privacy founded upon exclusivity may be a "culture-specific reflection of our possessive market-oriented society, rather than a universally necessary feature of social life".[31] The highly utilitarian notion that privacy is an essential precondition for an effective democratic society has also been disputed. For example, Richard Posner has argued that history does *not* teach that privacy as a precondition to creativity or individuality: the cultures of Greece, Renaissance Italy and Elizabethan England flourished in an atmosphere with much less personal privacy than is enjoyed today.[32] Likewise, the importance of privacy to values like love, friendship and trust is said to be overstated since privacy is "merely an imperfect substitute for information.[33] Indeed, a strict "law and economics" approach has led one commentator to conclude that an individual's interest in concealing embarrassing facts from the government is inefficient; society may be better off if such embarrassing information is disclosed.[34] Other social critics have complained of a "surfeit of privacy". In a highly individualistic society, in which there is an exaggeration of the private realm and neglect of the more public aspects of life, some individuals are alienated, lonely and scared.[35] Regardless of the wide disparity of views concerning the meaning and importance of informational privacy, computer technology has led to widespread concern in this domain. The legitimacy of this concern will now be considered.

III. THE PARTICULAR ISSUE OF COMPUTERS

From the time of the Domesday Book onward government has been demanding and recording data and gathering information about people and their activities. About 1750, the notion of a national census was revived for the first time since the Roman era. Modern census taking began in Continental Europe and then spread to North America. Probing by census takers for information about income, family life, living habits, and other personal matters initially met with public resistance and resulted in the creation of the so-called "statistical file" in which facts about specific individuals could not be discerned as readily.

The emergence of computerized data systems during the late 1950s and early 1960s led many government agencies and businesses to make their files machine readable. By the mid 1960's to about 1970, centralized computer services with data banks became a reality. Alan Westin foresees greater risks to information privacy in the near future as information systems become increasingly integrated. The spectre of a "womb to tomb" dossier raises uncomfortable overtones of a totalitarian society. Not only would such a file become easily accessible and retrievable, it

---

31. A. Schafer, "Privacy: A Philosophical Overview" in D. Gibson (ed.), *Aspects of Privacy Law* (Toronto: Butterworths, 1980) 1 at 16.

32. R.A. Posner, "The Right of Privacy" (1978) 12 *Ga. L. Rev.* 393 at 407.

33. *Id.* at 408.

34. *See* A.T. Kronman, "The Privacy Exemption to the Freedom of Information Act" (1980), 9 *J. Legal Studies* 727 at 760-66.

35. *See e.g.*, H. Arendt, *The Human Condition* (1958), 23-73.

would also be a very powerful instrument of surveillance and social control. In 1977, the U.S. Privacy Protection Study Commission concluded:[36]

> The substitution of records for face-to-face contact in these relationships is what makes the situation today dramatically different from the way it was even as recently as thirty years ago. It is now commonplace for an individual to be asked to divulge information about himself for use by unseen strangers who make decisions about him that directly affect his everyday life. Furthermore, because so many of the services offered by organizations are, or have come to be considered, necessities, an individual has little choice but to submit to whatever demands for information about him an organization may make. Organizations must have some substitute for personal evaluation in order to distinguish between one individual and the next in the endless stream of otherwise anonymous individuals they deal with, and most organizations have come to rely on records as that substitute.

It is traditional for Time Magazine to elect someone annually as the "Man of the Year". It may be ominous that on January 3, 1983 the computer was elected as "the machine of the year". The Canadian Privacy Commissioner, Inger Hansen, Q.C. has reported that "given sufficient resources it would be possible to build a single computer facility that would be able to store all information in existence today and that the information could be shared with anyone with the capacity to receive it".[37] Modern computer memories now exist that could generate a twenty page dossier on every man, woman and child in the United States with the maximum search time per file of four minutes.[38] Processing time has been greatly reduced and speed improved dramatically during recent years. Time sharing has allowed for greater efficiency and made central data processing centres accessible from remote terminals. It is now economical to use computers to retrieve relatively small amounts of information stored within much larger files.

Although computer-based information systems are now an essential feature of the corporate state, experts are divided on their impact on privacy. For example, Colin Tapper makes a provocative comparison by noting that the anonymity that was made possible by the installation of automatic telephone switching systems ensured greater privacy than was possible when the village postmistress was aware of every individual's telephone communications.[39] Moreover, dealing with aggregate data in a computerized form often guarantees greater privacy than was possible when the indentity of the individuals concerned was known to the researcher. However, in the past the major protection of the individual's privacy was the difficulty of access to large masses of data, stored in a variety of ways. Data had to be analyzed, sorted, collated and interpreted as one integrated set of related facts. Today's computers have the speed and the capacity to store, combine, retrieve and transfer data at comparatively low unit cost.

---

36. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington: U.S. G.P.O., 1977) at 4 - 5.

37. Inger Hansen, *Report of the Privacy Commissioner on the Use of the Social Insurance Number* (Ottawa, 1981), at 200.

38. *Supra* n. 12 at 167.

39. C. Tapper, *Computer Law* (2nd ed.) (1982) at 120.

The following summary lists some of the practical implications of this technology for privacy:[40]

1. Computers facilitate the maintenace of extensive record systems and the retention of data in those systems. Governments and those private institutions with the resources to utilize large storage of data have correspondingly enhanced powers over the individual;
2. They can make data easily and quickly accessible from many distant points. Security of remote terminals becomes a problem. This problem is enhanced by telephone linkage or satellite transmission of data;
3. They make it possible for data to be transferred from one information system to another. Many of the impediments initially encountered in integrating data systems have now been overcome;
4. They make it possible for data to be combined in ways which might not otherwise be practicable;
5. Because the data are stored, processed and often transmitted in a form which is not directly intelligible, few people may know what is in the records or what is happening to them.

There is also a concern that a computer printout is less likely to display the information gatherer's bias or selectivity than is a newspaper article or television report. There is higher probability that what appears as an unbiased computer report will be accepted as accurate whereas information in manila file folders may reveal erasures for insertions that are "invisible" on a computer screen.[41] More generally, the individual is increasingly pressured to perform "for the record" and becomes objectified as a object of computer manipulation. In addition, the persistence of a personal dossier on the individual makes it difficult to "make a fresh start". Since the cost of storing personalized data has dropped exponentially, the growth of decision-making "by the record" has augmented the danger that decisions will be made on the basis of erroneous information. It is often economically feasible to gather information which is not strictly relevant to the purpose of its storage.

Of course, many of these concerns relate neither specifically to privacy nor to a computerization of personal information. Newer technology such as optical scanners can minimize inaccurate data. Often complaints about inaccuracy in data merely camouflage differences in opinion or relate to alleged incompleteness.

A. SECURITY OF COMPUTERIZED RECORDS

The confidentiality of data depends on both physical and intangible barriers. Physical barriers may consist of walls and locks of varying sophistication protecting computer terminals. Data encryption constitutes another physical barrier. Intangible barriers depend upon influencing human behaviour through training or sanctions. Intangible barriers may also be created by laws against disclosure of particular kinds of information, punishable by penalties of varying severity.[42] In British

40. This list is derived from A. Goldworthy, "Learning to Live with the Computer", in *Occasional Papers* (1977) at 12.
41. *Report of the Commission of Inquiry into the Confidentiality of Health Information* (the Krever Commission) (1980), volume 2 at 162.
42. *E.g.*, Officials Secrets Act, R.S.C. 1970, c. 0-3; Venereal Disease Act, R.S.B.C. 1979, c. 422.

Columbia, where all provincial government data processing is centralized in a Crown Corporation, an employee of the Crown Corporation who wrongfully discloses confidential information may not only be dismissed and fined, he or she is also liable to an aggrieved individual or to the Crown for damages.[43] There are privileges against the disclosure in court of certain information arising in particular contexts. Professional codes of ethics may also bolster confidentiality.

Computer security can be penetrated by both "outsiders" and by the "insiders", who have been authorized to use the data. Of course, "insiders" represent a greater danger than "outsiders". Even sophisticated data encryption systems are not foolproof: the better the locksmith, the better the lockpicker usually becomes. Time sharing also increases the danger that outsiders will penetrate the system. Satellite transmission makes information particularly vulnerable.[44] It has recently been reported that computers "whisper" their data by emitting radio waves from screens, wiring and power lines, which can be decoded.[45] An excellent illustration of Canadian concerns over data confidentiality is provided by the so-called Dalton School Caper. In 1980 a number of Grade 8 students from a New York private school attempted to tap into twenty-one Canadian data banks. Files were destroyed in several of the firms invaded by telephone, and security systems were broken in private firms, universities and federal data banks which allowed dial-in access.

Despite such chilling examples of inadequate protection, concerns over computer security are often exaggerated. Many problems can be eliminated simply by better physical security for computer records. Special passwords may be utilized effectively and data encryption is a rapidly developing science: a "technological fix" may yet solve the computer security problem. However, privacy safeguards are expensive. Incentives must be given for their use; in government and in the private sector. It is most important that specific judgments be made about the degree of protection required for various kinds of data. For example, certain information in government data banks such as records of vaccinations may require only minimal safeguards since their value to the individual's privacy is normally quite low. Other information such as medical records and details of mental problems must be kept private, even at substantially greater costs for data security.[46]

Whatever the reality of present computer security, there is no doubt that the public *perceives* increasing computerization as a threat to privacy. Moreover, polls indicate that privacy concerns have increased significantly in recent years.[47] Surveys have also shown that the protection of privacy should not be interpreted as a predominantly middle-class

43. System Act, R.S.B.C. 1979, c. 399, s. 19.

44. For a good summary of current developments, *see* B. Harrison, "Data Security: Plan for the Worst" in *Infosystems* (June, 1982) at 52.

45. "Computer 'Whispers' Worry Washington", Globe & Mail, April 9, 1983.

46. This was one of the central recommendations of the Krever Commission. Report of the Commission of Inquiry into the Confidentiality of Health Information (1980), recommendation 36, volume 2, at 179.

47. *See, e.g.*, Ontario Commission *supra* n. 13 at 507 - 510.

concern.[48] Even if computerized files are actually more secure in large systems than when scattered, the breach of a centralized information bank would net so much more confidential information that the threatened harm is indeed much greater. The extent and nature of the personal information stored in modern government information banks is well documented by the Ontario Commission on Freedom of Information and Individual Privacy.[49] Birth, death, health, business, welfare, professional status, property, child welfare and criminal matters are just some examples of the types of often sensitive information now found in government data banks.

IV. THE CANADIAN LEGAL RESPONSE

A. INTRODUCTION

The public's concern to safeguard the personal information kept in institutional data banks has prompted various reform proposals. Westin and other critics have long proposed that the operation of personal data systems be subject to some regulatory control. The obvious efficiency gains made possible by computer technology must be weighed against certain costs to individual privacy which must be incurred. It is obvious that the value of informational privacy cannot be absolute; it must be weighed against competing public goods.

To an economist the privacy debate may be viewed as an attempt to formulate the appropriate legal definition of ownership and property rights in personal information.[50] It is suggested that these property rights could be allocated in several ways. At one extreme, individuals could be given exclusive rights to personal information preventing anyone, including the government from obtaining it without their approval. At the other extreme, all personal information could be public. It is obvious that some middle ground must be achieved if such normal government functions as education and income redistribution are to be performed effectively. The government must have coercive powers to acquire certain types of information.

One method of grappling with the issue of privacy in computers is to utilize the criminal sanction. Obviously if interference with information banks and stealing confidential information were adequately treated by the criminal law, there would be less concern about informational privacy. However, courts have held that confidential information is not property for purposes of the law of theft in Canada.[51] When computers are abused and individual privacy invaded, present criminal law remedies are sadly outdated. Recently the Canadian House of Commons Committee on Justice and Legal Affairs endorsed most of the recommendations

48. *See* A. Neier, "Privacy, Society and Dossiers" in Grant S. McClellan, (ed.) *The Right to Privacy* (1976), at 15 - 17.

49. Ontario Commission, ch. 27. *See* also M. Brown *Privacy and Personal Data Protection* (Toronto: Commission on Freedom of Information and Individual Privacy, Research Publication 15, 1980).

50. *See* Roger Noll, "Regulation and Computer Services" in M. Dertouzos and J. Moses, *The Computer Age: A Twenty Year View* (1980) at 254.

51. "I conclude that confidential information is not property for the purpose of the law of theft in Canada". *R.* v. *Stewart* (1982) 68 C.C.C. (2d) 305 (O.H.C.) (*per* Krever, J, at 316).

of Bill C-667 which would amend the Criminal Code and the Canada Evidence Act[52] with respect to computer crime.[53]

In an Alberta case,[54] two students and a part-time employee gained access to a computer without authorization. They examined some university data, interfered with the input of data and acquired the confidential passwords of other users. A charge of theft of telecommunications services under s. 287 of the Criminal Code was dismissed when the court held that a computer system was not a telecommunication facility. Legislators must be very cautious if the criminal remedy is to be applied effectively in the computer context. For example, to define all information stored in a computer as property for the purpose of a charge of theft, would be using a rather blunt instrument to solve the problem. Likewise, if information is to flow freely in society, a general crime for invasion of informational privacy in the computer context would create serious difficulties.

B. THE REGULATORY APPROACH

1. Principles of Fair Information Practice

Varying reform proposals of a more explicitly regulatory nature have been advanced in North American and European jurisdictions. Although they vary widely with the political and social mores and legal traditions in each jurisdiction, they are all designed to enhance the individual's control over personal information collected by institutional record keepers. "Fundamental principles of fair information practice" were first articulated in a 1973 U.S. Government report and have been very influential in most reform efforts.[55] They may be summarized in the following terms:

1. There must be no personal data record-keeping systems whose very existence is secret;
2. There must be a way for an individual to find out what information about him is in a record and how it is used;
3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent;
4. There must be a way for an individual to correct or amend a record of identifiable information about him;
5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[56]

The Privacy Protection Study Commission has added two further principles to this list:

6. Unnecessary cost to the requestors of personal information should be avoided as far as possible;
7. Additional or new institutional arrangements should be devised for the prompt and informal redress of personal information grievances.[57]

---

52. Canada Evidence Act, R.S.C. 1970, c. E-10.
53. Vancouver Sun, June 30, 1983.
54. *R.* v. *McLaughlin* [1980] 2 S.C.R. 331.
55. The Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens* (1973).
56. *Id.* at 41.
57. Privacy Protection Study Commission, *supra* n. 36 at 30.

It is against this list of reform principles that the Canadian legal response to informational privacy concerns will be evaluated.

One alternative to traditional government regulation may be to create a body of law that makes privacy rights explicit. Roger Noll has argued that the ultimate source of the demand for privacy "rights" has arisen from the failure of legislatures and courts to develop such a body of law.[58] In Commonwealth nations, the common law offers no protection for personal privacy *per se*.[59] In Quebec, article 1053 of the Civil Code has been interpreted to provide some protection for personal privacy. The 1968 Report of the Quebec Civil Code Revision Office has proposed the adoption of an article which would categorically state a right to privacy.[60]

Protection from data surveillance and the unreasonable compilation and use of data relating to individuals have not been enhanced by developments in tort law. The court's equitable jurisdiction to prevent a breach of confidence may, in certain instances afford some protection in this regard. Although some scholars believe that this cause of an action is still at an embryonic state,[61] the English Younger Committee Report has recommended that the Law Reform Commission consider modifications to the law of breach of confidence to provide better protection for informational privacy.[62]

The Provinces of British Columbia,[63] Manitoba,[64] and Saskatchewan[65] have enacted Privacy Acts. Professor Burns has reviewed the jurisprudence and concluded that the legislation is a "nondevelopment".[66] Other legislation has placed limits on the uses of certain types of information collected by government. Confidentiality guarantees are provided for census responses,[67] income tax returns[68] and for data relating to certain social diseases.[69] At lease one provincial Human Rights Act contains an explicit right to privacy.[70] During the debate over the passage of a Canadian Charter of Rights and Freedoms, the Progressive Conservatives pro-

58. Noll *supra* n. 50 at 266.

59. For an excellent canvass of the common law position, with particular reference to Canada, *see* P. Burns, "The Law and Privacy — The Canadian Experience" (1976), 54 *Can. Bar Rev.* 1.

60. *See*, generally, H. Patrick Glenn, "The Right to Privacy in Quebec Law" in D. Gibson (ed.), *Aspects of Property Law* (1980) at 41 - 71.

61. Dr. Morison in *Report on the Law of Privacy* (N.S.W. Government Printer: Sydney, 1973) at 295.

62. Report of the Committee on Privacy (1972), Cmnd. 5012 at 295.

63. Privacy Act, R.S.B.C. 1979, c. 336.

64. The Privacy Act, S.M., 1970, c. 74.

65. Privacy Act, R.S.S. c. P-24.

66. Burns *supra* n. 59 at 33.

67. Statistics Act, S.C. 1970-71-72, c. 15, s. 33.

68. Income Tax Act, R.S.C. 1952, c. 148 as amended, s. 241.

69. Venereal Diseases Act, R.S.B.C. 1979, c. 422, s. 12.

70. Article 5 of the Quebec Charter of Human Rights and Freedoms, S.Q. 1975, c. 6 provides that "Every person has a right to respect for his private life". This guarantee, however, is generally interpreted as merely declaratory.

posed entrenching a right to privacy such as is found in the constitutions of certain American states.[71]

2. Some Alternatives

The Canadian government considered a wide range of legislative options which have emerged elsewhere to decide how to tackle the issue of informational privacy specifically. The American Privacy Act[72] is at one end of the spectrum. Although it is designed to impose a code of fair information practices along the lines outlined above,[73] it is self-regulatory in nature: individuals must enforce rights created under the Act against federal agencies on their own initiative. For example, the right of access to federal information banks can be asserted in the courts, but only at the behest of the individual citizen. The court may order the federal agency in question to release information and has the right to inspect all information banks in order to make its determination.

At the other extreme, there is the approach represented in the proliferation of data protection agencies in Europe, several of which have very extensive regulatory powers.[74] For example, the Swedish Data Inspection Board is a supervisory agency created by statute with very extensive powers to regulate all aspects of data collection, storage and access in both the public and private sector. In Australia, the New South Wales Privacy Committee presents another very different approach. It was created by statute in 1975.[75] The Committee does not enforce a general legal right to privacy but rather attempts to mediate disputes and to recommend specific law reform, if and when it appears necessary. The low-key mediation approach in New South Wales appears to have been successful in resolving almost all complaints and securing voluntary adoption of codes of behaviour.

During the period between its establishment in 1975 and end of June 1978, the Committee actively investigated almost 900 complaints. In only two cases were the Committee's recommendations rejected.[76]

3. Canadian Initiatives

What has been the Canadian response to this wide variety of legislative initiatives abroad? It is perhaps monotonous though necessary to begin all discussions of regulatory reform in Canada by reference to the division of powers between the federal and provincial governments under the Constitution.[77] The release of the Report of the federal government's Task Force on Computers and Privacy in 1972 led to considerable discussion between federal and provincial authorities on data exchange and the

---

71. *See, e.g.*, California State Constitution, which was amended in 1972 to provide the individual with a "legitimate expectation of privacy": *Burrows* v. *Superior Court* 13 Cal. 3d 238 (1974).

72. U.S.C.A., s. 552a.

73. Text accompanying notes 56, 57 *supra*.

74. *See* Bing, "A Comparative Outline of Privacy Legislation" (1978), 2 *Comp. L.Y.B.* 149.

75. Privacy Committee Act, 1975, No. 37 (N.S.W.).

76. Ontario Commission, *supra* n. 13 at 638.

77. Constitution Act, 1867, ss. 91, 92.

standardization of legislation amongst various government jurisdictions. However, no consistent computer data policy emerged in Canada, perhaps, in part, because public opinion simply was not aroused enough to force the hand of all governments in the country.

The central government could not act alone to develop such a policy due to the lack of a clear constitutional jurisdiction over the issue. Canada's first venture into data protection legislation was the passage of Part IV of the Canadian Human Rights Act[78] which was finally proclaimed on March 1, 1978. Despite Ottawa's hope that its policies respecting federal government data banks would be copied at other levels and that procedures would be harmonized,[79] only Quebec has followed suit with similar legislation designed to protect personal information in government files.[80]

The scope of federal jurisdiction over informational privacy is unclear. Privacy *simpliciter* falls largely under provincial jurisdiction. The federal government would enjoy legislative competence over extra-provincial computer data banks. Mr. Fred Jordan, Q.C. has concluded that:[81]

> The scope of the federal power over the protection of privacy in relation to computer-oriented information systems appears to be primarily a factor of the degree to which computers evolve as an integral part of the Canadian telecommunications system. The issue of the regulation of telecommunications within a province is currently in dispute. Federal power would also be limited in relation to the data gathering phase of computerization unless data gathering can be characterized as an integral part of the computer data bank operation.

Parliament may also exercise some power to safeguard privacy by virtue of its legislative jurisdiction over such heads of power as statistics, banks and criminal law. The major area of Parliament's jurisdiction is its power over extra provincial works and undertakings. If a computer data bank operation is confined to the boundaries of a province, however, the provincial legislature will have the primary regulatory authority in this field.

4. The Canadian Privacy Act

On July 1, 1983 the Canadian Privacy Act was proclaimed.[82] This Act replaces Part IV of the Canadian Human Rights Act which was entitled "Protection of Personal Privacy". In many ways the new Act builds on the experience gained under its predecessor. In general, four rights were provided in the Canadian Human Rights Act to Canadians and others lawfully admitted to Canada for permanent residence. They were as follows:[83]

> 1. The right to know what records were used for administrative purposes concerning them which were held by federal departments or institutions listed in a Schedule to the Act.

78. *Supra* n. 10.

79. However, the Government of Ontario is currently considering the Report of its Commission on Freedom of Information and Individual Privacy which strongly recommends the statutory implementation of fair information practices (*see*, Chapter 32 Ontario Commission Report).

80. Bill 65, (An Act respecting access to documents held by public bodies and the protection of personal information) was assented to on June 23, 1982.

81. *See* F.J.E. Jordan, *Privacy, Computer Data Banks, Communications and the Constitution* (A Study for the Privacy and Computers Task Force) (1972).

82. *Supra* n. 11.

83. *See* also *Annual Report of the Privacy Commissioner* (1980) at vii.

2. The right to know uses made of such information since 1 March, 1978.
3. The right to examine such personal information as well as the right to challenge its accuracy and completeness and to require a notation on a file when a correction is not accepted.
4. The right to be consulted in respect of proposed uses, for administrative purposes, of information provided to the federal government by an individual for a different, unrelated purpose, when such uses were not authorized by law.

The Act requires the publication of an annual index describing all "federal information banks". The Index to Federal Information Banks lists over 1500 such banks. The Act provided that complaints about violation of these rights could be taken to a Privacy Commissioner for investigation. Ms. Inger Hansen, Q.C. was appointed under the Act with authority to make recommendations to federal government institutions in an effort to settle complaints. Mr. John Grace has replaced Ms. Hansen as Privacy Commissioner under the new Privacy Act; Ms. Hansen has become the Information Commissioner under a companion statute, the Access to Information Act.[84]

The Treasury Board, the federal government agency primarily responsible for financial administration, was authorized to oversee the future collection and storage of personal information. In doing so, the Treasury Board published an elaborate set of guidelines designed to ensure compliance with the Act's objectives.[85] Although these directives did not have the force of law, the Treasury Board had indicated that they were to be adhered to unless the Board consented to a particular exception. Finally, the Act set out detailed exemptions which could be claimed in respect of the rights provided. Individual files or parts thereof could be exempted and entire information banks were excluded from some of the rights granted in the Act. Twenty-two such banks were exempted by order of the Minister responsible with the approval of the Governor in Council.[86] The grounds for such exclusion referred to information which, if released, could damage international relations, federal-provincial relations, national defence or security, suppression of crime, and the investigation of offences under federal laws.

The Privacy Act is very similar to its predecessor in each of these respects. Nevertheless, there have been some significant changes made. The scope of the "exemptions" — the exceptions to the right of access — are somewhat more limited in the new Act. The glaring exception to this rule is the fact that the new Act does not apply at all to personal information found in any Cabinet documents.[87] The powers of the Privacy Commissioner are expanded considerably in the new legislation. If the Commissioner is unable to effect a settlement with the government institution in question, he will now be able to recommend judicial review of the government's decision to withhold certain information.

The Commissioner may receive or initiate complaints on a variety of subjects including the collection, retention or disposal of personal in-

84. S.C. 1980-81-82, c. 111.

85. *See* Treasury Board of Canada, *Administrative Policy Manual*, c. 410, 415, 420 and 425 (December, 1978).

86. s. 53.

87. *Supra* n. 11, s. 70.

formation by a government institution, the unauthorized use or disclosure, wrongful disclosure of personal information, or the improper withholding of information under the Act.[88] As well, individuals may complain about failure to correct information which is believed to be erroneous. The Commissioner has the explicit power to carry out random audits of exempt information banks and make annual or special reports to Parliament on their status and the compliance by government with any recommendations made.[89]

A very significant addition to the Privacy Act is the right to seek judicial review of government decisions to withhold information.[90] If an individual has been refused access to personal information, he or she may apply for judicial review of this decision. Like the Commissioner, the Federal Court is empowered to look at any record to which the Act applies and in most instances the court may order its disclosure. However, for certain kinds of records the court is only empowered to order the disclosure "if it determines that the head of the institution did not have reasonable grounds on which to refuse to disclose the personal information".[91] This restriction on the court's powers on judicial review pertains to records coming within four exemptions in the Act:[92]

1. Federal-provincial affairs;
2. International affairs and national defence;
3. Law enforcement and penal security; and
4. Records which "could reasonably be expected to lead to a serious disruption of the individual's institutional, parole or mandatory supervision program".

Of course, the Federal Court may not examine any personal information contained in a Cabinet record since the Act does not apply to such information. The Act contemplates *ex parte* and *in camera* proceedings in certain circumstances.

A very practical right conferred upon the Privacy Commissioner is his ability to apply to the court for review of any refusal to disclose the record on behalf of a complainant or, alternatively, with the leave of the court, as a party to any review for which the complainant has applied.[93] In other words, the Privacy Commissioner may take important, precedent-setting cases at no cost to the complainant. Moreover, since the Commissioner has access to all documents whether or not contained in exempt information banks, his knowledge of their contents will be invaluable in litigation. In the United States, the understandable failure to grant an individual litigant or his counsel access to the contested information prior to the lawsuit has erected a formidable barrier to litigation under the American Privacy Act.

Therefore, how effectively does the new Privacy Act apply the principles of fair information practice outlined above?[94] Generally there are

88. *Id.* s. 29.
89. *Id.* s. 36.
90. *Id.* ss. 41, 42.
91. *Id.* s. 49.
92. *Id.* s. 24(a).
93. *Id.* s. 42.
94. *See supra*, text accompanying note 56, 57.

to be no secret personal data systems.[95] The Act itself places no limits on the types of personal information that may be gathered, and there are no rules relating to the collection process. However, the Act directs that no personal information shall be collected unless it "relates directly to an operating program or activity of the institution".[96] Wherever possible, the government institution shall collect information directly from the data subject.[97] Personal information shall not be disclosed without the consent of the individual except in circumstances listed in the Act.[98] Information acquired for one purpose may only be used for uses consistent with that purpose.[99]

Although personal information may be made available to certain investigative bodies, the Privacy Commissioner must be informed of requests for such information. In other cases where a government institution proposes to release personal information when it considers that "the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure", the Privacy Commissioner is to be informed and he may notify the individual concerned.[100] When information is used for purposes other than that for which it was obtained, the Privacy Commissioner shall likewise be notified. The Treasury Board has also published a mandatory directive which states that "in the course of collecting information for inclusion in a bank of information, data sources shall not be given the impression that a response is mandatory unless response is legally required".[101]

Under the Act an individual is entitled to obtain access to personal information and request correction or notation of a requested correction if the record is not amended.[102] Although the Privacy Commissioner may investigate all such complaints, judicial review is only available in cases where access has been refused. It is most regrettable that judicial review of government practices with respect to the collection, retention and disposal of personal information is not likewise permitted. For example, since the Act assumes that the unauthorized collection or linkage of personal information may infringe serious rights of the individual, it would be consistent to permit judicial review and perhaps injunctive relief to enjoin any such abuses. Moreover, the Privacy Commissioner does not have the same unfettered discretion to initiate investigations of these governmental practices as he enjoys with respect to exempt information banks and the use of the personal information. Only if he has "reasonable grounds" may he investigate these matters on his own initiative.[103]

95. However, s. 16(2) allows all government institutions to refuse to indicate whether personal information exists. Although perhaps justifiable in a narrow range of national security matters, the provision if not limited in any way and could be the subject of abuse.

96. s. 4.

97. s. 5.

98. s. 8(2) contains a list of 13 situations in which confidentiality may be legally violated.

99. s. 7.

100. s. 8(2) (m)(i), s. 8(5).

101. Treasury Board, *op. cit.* at 11. This directive pertained to Part IV of the Canadian Human Rights Act. Treasury Board Directives under the Privacy Act are not available at the time of writing.

102. s. 12(2).

103. s. 29(3).

5. Unauthorized Linkage of Records

Like other data protection statutes, the Privacy Act imposes restrictions upon the transfer of records by the federal government. Information collected for one purpose is generally not to be made available for another purpose. For example, if financial information is provided in income tax returns, it should not be used for making decisions relating to unemployment insurance eligibility as this would not be a "consistent use" of the income tax information provided unless an Act or regulation specifically authorized the disclosure. When one provides information to the government for a particular purpose, the Act would permit that this information to be used for other purposes only if the individual consents or if the second purpose is "consistent" with the original purpose for which the information was provided.[104] The Index to Federal Information Banks must provide "a statement of the uses consistent with such purposes for which the information is used or disclosed".[105]

However, the Act lists many circumstances in which personal information controlled in one information bank may be disclosed for other purposes. For example, certain investigative bodies may receive such information "for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation" if a written request is forwarded to a particular bank.[106] No judicial warrant is required. As the Canadian Civil Liberties Association has noted in its testimony to the Justice and Legal Affairs Committee considering this legislation:[107]

> It is rare when the law permits investigative agencies to invade residential privacy without a judicial warrant. Why should the law permit such agencies to invade *information* privacy without an analogous safeguard? The adoption of such a safeguard would help to ensure that proper grounds existed before such extraneous uses could be made of personal information. The "tunnel vision" so often associated with investigatory agencies should be made subject, where possible, to an independent evaluation. Apart from situations of imminent peril to life or limb, such disclosures should require a judicial warrant.

It should nevertheless be noted that the McDonald Commission of Inquiry into R.C.M.P. practices criticized this provision as going too far in opening up access and confidential information to investigative bodies such as the R.C.M.P.[108] The Report complained that there was not a clear enough test of necessity for access to personal information contained in the section in question. The Report also called for a distinction between information about a person which is publicly available, such as biographical information and information which is not publicly available. On the other hand, the Commission criticized the legislation for not providing access to certain kinds of information such as income

---

104. Unfortunately, the Act contains no definition of what constitutes a "consistent use".

105. Section 11(1)(a)(iv). It appears that these stipulations apply to information collected from third party sources or from other government sources and do not apply solely to information submitted by the data subject. The forerunner provision, s. 52(2) of the Canadian Human Rights Act, appeared to apply onto to data submitted by the individual concerned.

106. S. 8(2)(e).

107. *Minutes of proceedings and evidence of the Standing Committee on Justice and Legal Affairs*, (32nd Parl., 1st Sess.), (1980-81), 23A:13.

108. *See* Commission of Inquiry Concerning Certain Activities of the *Royal Canadian Mounted Police* (1981) at 1028.

tax, family allowance, old age security and Canada Pension Plan information.

In each case the information in question is shielded from disclosure under various Acts of Parliament. Accordingly, the Commission recommended that routine "biographical information" should be made available for criminal investigation purposes and for security intelligence. However, the Commission made the following important recommendation:[109]

> All other personal information held by the federal government with the exception of census information held by Statistics Canada [should] be accessible to the R.C.M.P. through a system of judicially granted authorizations subject to the same terms and conditions as are now found in s. 178 of the Criminal Code with respect to electronic surveillance.

Perhaps the most controversial category of disclosure authorized under the Privacy Act entitles personal information to be disclosed:[110]

> . . . for any purpose where, in the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure.

A complementary provision in its companion statute, the Access to Information Act, reiterates that personal information may be disclosed in accordance with this provision.[111] The American legislation also contains a balancing test for determining circumstances in which personal information may be released.[112]

It is disturbing that the opinion of the government official is to be final in the Canadian Act. Indeed the decision of the official is not even restrained by any "reasonable grounds" test. There is no requirement that the individual concerned be notified of a government decision to disclose information, although he or she has the right to complain to the Privacy Commissioner. There is no right to seek judicial review of a Privacy Commissioner's recommendation in this regard.

6. The Social Insurance Number and Data Linkage

The creation of a single identifying number for all citizens in a country has been a matter of continuing concern. As more records are kept for individuals, and for longer periods of time, standard identifiers such as names and addresses are increasingly inadequate. As large record systems are increasingly computerized a "unique personal identifier" eliminates cross-checking and improves search efficiency. Incidentally, such numbers may have advantages in privacy protection because one individual is less likely to be confused with another with a similar name or address. Most citizens have several personal identifier numbers as a result of the various government records, bank records, credit cards and so forth which are accumulated. When the same number is used by several

---

109. Recommendation 271 at p. 1029. The much criticized Canadian Security Intelligence Service Act, Bill C-157 embraces this recommendation but would allow access to *all* personal information, including census records [s. 22(1)].

110. s. 8(2)(m)(i).

111. Access to Information Act, S.C. 1980-81-82, c. 111, s. 19(2).

112. 5 U.S.C., s. 552 (b)(6). The leading case is the *Department of the Air Force* v. *Rose* 425 U.S. 352 (1976).

government agencies and by the private sector, the possibility of data linkage arises, with the attendant concern of privacy invasion. For many years the spectre of a "womb to tomb" dossier being available to public and private organizations has been raised.

There are several advantages resulting from the use of a single identifying number. By definition, greater accessibility to personal information systems is promoted. Without physically linking data banks, information in several different systems may be merged. As a result, the data base available for government decision-making is increased and there is less duplication in the collection of information. The individual may benefit by more accurate record keeping and by a simplified task in retrieving personal information and controlling its use.

On the other hand, significant costs and risks may be incurred if a single identifying number is created. Many are concerned that a unique, permanent number would facilitate tracing an individual, monitoring one's behaviour and controlling it. Routine access to all the records compiled for one individual would make it indeed difficult for one to "pull up stakes" and make a fresh start. The government would have a strong incentive to issue identity cards featuring this all important number. Already so-called "smart cards" are available which contain a computer chip recording all of one's medical history, driving record, library status and so forth. The general dehumanizing influence of a single identifying number is perhaps the greatest concern that is usually voiced.

The issue of data linkage, by which information collected for one purpose is used for another has already been examined. A single identifying number would enhance the ease with which data may be shared. In Canada, the Social Insurance Number (S.I.N.) has been in use since 1936. In 1965 the S.I.N. was adopted for use in tax collection and pension payment under the Canada Pension Plan.[113] The federal government promised that the S.I.N. would be used only for these purposes. Information available with a S.I.N. included the name, address, employment records, date of birth, mother's name and province of origin. The actual S.I.N. card contains only the individual's signature and a nine-digit number.

Over the years, many of the concerns initially expressed by members of the Opposition in Parliament concerning the proposed uses of the new numbering systems have materialized. Among the uses reported by Inger Hansen, the Privacy Commissioner in her 1981 Report on this issue, were the following:[114]

> In the federal government's sphere the number is required on a long list of forms, ranging from employees' travel claims to requests for access to personal information banks, and applications for participation in the annual goosehunt; in provincial jurisdictions, on lists of electors or applications for fishing licences, and in the private sector, it may be required to cash cheques or to rent a vacuum cleaner.

The R.C.M.P. has had almost unlimited access to the central S.I.N. index and has used it extensively to track down suspects. In fact, in 1969 the R.C.M.P. was given a telex number to call up information from the

113. Canada Pension Plan Act, S.C. 1965, c. C-15, s. 100.

114. Privacy Commissioner, *Report of the Privacy Commissioner on the Use of the Social Insurance Number* (Ottawa: 1981), at p. 2.

Unemployment Insurance Commission's central computer index. The McDonald Commission was informed that a secret agreement was signed in 1974. Other users of the social insurance information have included the Ontario Provincial Police, The Quebec Provincial Police, National Revenue, National Defence, British Customs and the Indiana State Police. Various federal agencies have used the number to cross-check personal information submitted to them.[115]

Despite the widespread use of the S.I.N. the Privacy Commissioner concluded that data linkage was not widespread. However, she expressed no doubt that the number could potentially be used as a universal identifier and for data linkage purposes. She concluded that prohibiting the collection and use of the social insurance number would have little effect on sharing information between computer banks, since the technology for data linkage had advanced so rapidly that a single identifier would no longer be critical in facilitating the merger of computerized files.

Among the recommendations on the use of the S.I.N. advanced by Ms. Hansen was that the federal government inform citizens of their rights to be exempted from being identified by a S.I.N. or other number.[116] In addition, the government must terminate the use of an individual's S.I.N. if the individual pays a fee for part of the increased costs imposed by the individualized processing of personal information. This recommendation would appear to be administratively unworkable and, ironically, the increased attention focussed upon those individuals seeking exemption might augment their privacy concerns.

The more general issue of data linkage, however, remains controversial. For example, Mr. Jan Freese, Director-General of the Data Inspection Board of Sweden has staunchly resisted the unauthorized linking of personal files, even if it could be demonstrated to have a socially useful purpose such as helping to convict welfare cheaters. Not only are privacy concerns paramount, in his view, the merger of information provided for different purposes may lead to misleading results. On the other hand, as Colin Tupper illustrates from actual English case histories, the linking of information banks may thwart serious crimes, such as occurred, when a former mental patient registered as a foster parent and subsequently murdered a child entrusted to his care.[117] If merger of information banks were always to be prohibited, it would be impossible to detect such tragic situations before they occurred. The blanket prohibition of data linkage is clearly unacceptable; instead, specific criteria for specific situations must be developed.

7. The Issue of Costs and Benefits

The two additional principles of fair information practice suggested by the U.S. Privacy Protection Commission will now be addressed. The

115. *See* K. Rubin, *How Private is Private? Some Experiences and Accounts About Federal Information Privacy Policies* (Ottawa: Canadian Federation of Civil Liberties and Human Rights Associations, 1978).

116. Report of the Privacy Commissioner on the Use of the Social Insurance Number, *supra* n. 114 at 231.

117. C. Tupper *supra* n. 39 at 124.

issue of cost to the requestors of personal information is a thorny one. Under the Access to Information Act proclaimed at the same time as the Privacy Act, an individual must pay an initial fee of $5.00 when invoking the legislation. This fee is intended to deter frivolous but costly requests for information. It entitles the applicant in theory to five free man-hours of government time. Thereafter, the applicant is charged $10.00 for each hour, plus $16.50 a minute for computer time and $20.00 an hour for computer programming time.[118]

By contrast, there is no charge for those who request personal information under the Privacy Act. Some economists would argue that personal information represents valuable property for the individual, just as the private information of corporations such as trade secrets or other corporate financial information can have very great value to these institutions.[119] In addition, as noted above, an invasion of one's informational privacy may be defined as a loss of the value of that privacy.[120] When control is lost over one's personal information many of the explicit and implicit costs which motivated legislative reform come into play. As a result, it may be argued that individuals should be expected to bear the brunt of protecting their valuable property interests in personal privacy as a measure of cost internalization. Nevertheless, the costs to the individual of enforcing privacy rights in government information banks are usually very high relative to the value of the personal information in question.

In the United States, the Privacy Act is largely self-enforcing. When information is wrongly denied under the Act, an individual must resort to the courts to vindicate privacy rights, incurring attorney fees and litigation costs which in most cases would be greater than the privacy values vindicated. However, the U.S. Privacy Act specifically overrules normal Americal civil practice by permitting the courts to assess "reasonable attorney fees and other litigation costs reasonably incurred . . . [when] the complainant has substantially prevailed".[121]

Within the government, of course, substantial costs are incurred in providing these rights to privacy. For example, in 1977 the U.S. Office of Management and Budget (C.M.B.) estimated that start-up costs in the first nine months after the Privacy Act had passed and the date it became effective were $29,459,000.00. First year operating expenses were an additional $36,599.00.[122] Comparative figures in Canada are, of course, not yet available for the recently proclaimed Privacy Act. However, the President of the Treasury Board, the Hon. Herb Gray, has proposed that the combined budget of the Privacy Commissioner and of the Information Commissioner be $2.8 million.[123] The actual costs incurred within the government institutions subject to the Privacy Act are difficult to

118. *Globe and Mail*, June 3, 1983, p. 1.

119. *See* R. Noll, *supra* n. 50 at p. 267.

120. *See* Parker, *supra* n. 22 at 284-88.

121. U.S.C. s. 552a (2)(B).

122. These figures are found in the Ontario Commission, *supra* n. 13 at 620.

123. Parl. Deb., (June 23, 1983) at 26719.

calculate, but must include the opportunity cost of the time expended by public servants in complying with the new law.[124]

The costs of safeguarding informational privacy must, however, be weighed against the less tangible benefits which emerge from data protection laws like the Privacy Act. In cost-benefit analysis, hard numbers like cost figures often dwarf soft variables like the improved public confidence in government. The latter values are indeed difficult to quantify as readily as information concerning cost, but must nevertheless be considered. The benefits accruing to society from the wholesale invasion of individual privacy will usually appear more compelling than the comparatively abstract value of privacy for individuals. As S.I. Benn has cautioned:[125]

> . . . privacy is a particularly vulnerable interest; in any given case, it is the interest of one individual or a relatively small group, while against it are set the interests of the public in being fully informed, in security from crime, in having policy-makers and administrators of the national economy, or [the public health insurance scheme] or city plans work with full and up-to-date information. Consequently, in any given instance, the public interest will seem overriding; yet in the long run protection of the interest of every individual in privacy will have gone by default; the piecemeal erosion of the privilege may never have been halted, to take an overall view of the total consequences. In this respect privacy resembles environmental values; the particular damage rarely seems sufficient to outweigh the promised benefits, but the cumulative consequences may be disastrous.

The second recommendation of the Privacy Protection Commission was that new institutional arrangements should be devised to promptly and informally redress personal information grievances. In this respect, the Canadian legislation would appear to be a significant improvement over its American counterpart. The Index to Federal Information Banks is widely available in post offices and libraries across the country. A simple form is available for requesting access to personal information contained in the information banks. However, even if the individual cannot locate the information in the Index, he or she now has the right of access to personal information if able to "provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution".[126]

The Act stipulates that the Privacy Commissioner must investigate all complaints before any litigation is permitted. If the Privacy Commissioner concludes that information is being wrongly withheld by a government institution he has the right to apply to the Federal Court on behalf of the complainant, at no cost to the complainant.[127] The Act also requires that the Federal Court dispose of cases brought under the Act "in a summary way, thereby reducing litigation expenses for the individual concerned.[128] Moreover, the costs of litigation normally follow the event in Canadian practice, and courts have considerable discretion regarding costs irrespective of the outcome of the suit. By way of conclusion,

124. R.C. Goldstein, *The Cost of Privacy*, (1974); V. Block, "Is Privacy Legislation a Bargain?" *Infosystems* (July, 1981) at 97.

125. S.I. Benn, *supra* n. 21 at 691.

126. s. 12(1)(b).

127. s. 42.

128. s. 44.

therefore, the Canadian legislation squares quite well with the recommended principles of fair information practice.

V. CONCLUSION

Throughout history society's knowledge about new technology consistently has grown more rapidly than its grasp of the consequences of that technology. Reaction to the emerging information society and its computer infrastructure is mixed. Optimistic forecasters, such as Mr. Yoneji Masuda of Japan's Institute for the Information Society prophesy a "Computopia" in the near future.[129] Information "utilities" will allow everyone to obtain information, solve problems and create untold opportunities merely by connecting one's home terminal to the utility. Access to the information utility will be available to everyone at low cost, at any time or place. Problems associated with the new technologies will be mitigated by the application of a procedure for technology assessment by which wise choices will be made after a careful assessment of costs and benefits.[130]

Pessimistic observers also abound. Jacques Ellul and exponents of his views such as Laurence Tribe paint a bleak picture of technology as an all-pervasive, uncontrollable force that makes real political choice impossible. Tribe, for example, contends that any process of technology assessment is predicated upon a technological mode of reasoning and action.[131] Often by regarding the control of technology as an inherently insolvable problem, these critics are placed in practical agreement with those who do not regard the control of technology as an important problem at all.

Of course, no one knows whether optimism or pessimism over rapid technological change is warranted. Data protection laws represent only one answer to the set of problems raised by the information technology. Other problems include radical changes in the structure of the domestic economy, labour markets and education. There are also serious concerns that the increasing computerization of most institutions will agument international power imbalances and lead to system vulnerability.[132] The Canadian Privacy Act is one kind of regulatory mechanism designed to confront the issue of informational privacy. It applies only to government record-keeping, and only at the federal level.

It is much too early to evaluate the impact of the Privacy Act. The Act sets out a very general code of practice binding upon a wide range of government institutions in a wide range of situations. Perhaps a more specific set of regulations is required to address particular privacy issues arising in particular contexts. Perhaps private data banks should be licensed by a government agency which is required to assess the

129. Y. Masuda, *The Information Society as Post-Industrial Society* (1980) at 114, 146.

130. For a critical appraisal of this technique, *see* L. Tribe, "Technology Assessment and the Fourth Discontinuity: The Limits of Instrumental Rationality" (1973) 46 *So. Cal. L. Rev.* 617.

131. *Id.* at 650-657.

132. *See* Science Council of Canada Report Number 33, *Planning Now for an Information Society* (1982).

likelihood of invasions of privacy raised by private sector record-keeping. The Swedish Data Inspection Board, for example, has this sort of comprehensive regulatory mandate.[133]

More experience with the Canadian data protection statute will provide more insight into the need for such reforms. Fortunately, Parliament has recognized the need for continuous re-evaluation of the Privacy Act. In an unusual provision, Parliament stipulated that there must be a "comprehensive review" of experience under the Act within three years of its proclamation.[134] The Committee must report to Parliament shortly thereafter with specific recommendations for any reform it may consider appropriate. It is hoped that this Parliamentary review will provide an opportunity and a forum for public consideration of the privacy issues raised by the emerging information society in Canada.

133. *See* H. Burkert, *The Organization and Practice of Data Protection Agencies* (E.E.C.: Brussels, 1980).

134. Privacy Act, S.C. 1980-81-82, c. 111, s. 75(2).