Dalhousie Law Journal

Volume 23 | Issue 2 Article 1

10-1-2000

The Personal Information Protection and Electronic Documents Act: A Lost Opportunity to Democratize Canada's "Technological Society"

Tina Piper
Dalhousie University

Tina Piper*

The *Personal Information Protection and Electronic Documents Act*: A Lost Opportunity to Democratize Canada's "Technological Society"[1]

Bill C-6, more recently known as the Personal Information Protection and Electronic Documents Act, is promoted by the Canadian government as privacy legislation to protect Canadians' personal information. This paper explores that characterization and concludes that it is inaccurate and misleading. The problems that motivated a response by Parliament are the proliferation and commercial importance of personal information, concerns Canadians have about its uncontrolled use by the private sector and the inadequacy of existing law to address those concerns. However, the Act has not responded to these problems. There are several reasons for this, primarily the disproportionate and anti-democratic importance of business interests in the promulgation of the legislation and the characterization of privacy in market terms rather than in the language of human rights and long-term policy objectives. The Act's failure to achieve its substantive goals is demonstrated by comparing it with other models of privacy protection, such as the Privacy Charter proposed by the House of Commons Standing Committee on Human Rights, equivalent legislation in Quebec and the Australian Privacy Charter. Ultimately, the paper proposes solutions that would be more responsive to citizens' privacy concerns.

Le gouvernement du Canada affirme que le projet de loi C-6, mieux connu sous le titre Loi sur la protection des renseignements personnels et les documents électroniques, a pour but de protéger la vie privée des Canadiens. Tout compte fait, au dire de l'auteur, il s'agit d'une fausse représentation. Le Parlement du Canada a voulu réagir aux dangers que posent entre autres la prolifération des renseignements personnels jumelée à leur valeur commerciale croissante, l'inquiétude du citoyen quant à l'exploitation débridée de cette information par le secteur privé et enfin l'impuissance du cadre législatif face à cette évolution. Cependant, le projet de loi C-6 n'apporte pas les solutions voulues au problème et cela pour plusieurs raisons. Sans doute d'abord parce que les intérêts privés qui préconisent haut et fort la promulgation de cette loi sont par nature anti-démocratiques et ensuite parce que l'on asservit la notion de vie privée à des impératifs d'économie de marché au lieu de l'envisager dans le contexte des

* L.L.B. Dalhousie Law School. Many thanks to Torys for funding to complete this paper through the J.S.D. Tory Writing Award. Special thanks to Teresa Scassa whose instruction and encouragement inspired this paper, and to David Piper, Audrey Macklin, Archie Kaiser and an anonymous reviewer for their insightful suggestions and comments.

1. I have borrowed the concept of "The Technological Society" as developed by Jacques Ellul in his influential book of the same name (New York: Alfred A. Knopf, 1964).

droits de la personne et des objectifs d'une politique à long-terme. Pour se convaincre que le projet de loi C-6 n'arrive pas à la cheville des objectifs auxquels il prétend répondre, il suffit de le comparer à d'autres modèles de protection de la vie privée tels que la charte sur le respect de la vie privée proposée par le Comité permanent de la justice et des droits de la personne, de la Chambre des Communes, la législation équivalente au Québec et enfin la charte sur le respect de la vie privée de l'Australie. Nous proposons en définitive des solutions qui répondraient mieux aux préoccupations des citoyens canadiens.

Introduction

I. *The Collection of Personal Information in Canada*

1. *How Personal Information is Collected*

2. *What Type of Personal Information is Sought?*

3. *The Purposes of Collecting Personal Information*

4. *Concerns Over the Collection of Personal Information*

II. *The Underlying Privacy Protection Framework*

1. *The Legal Protection of Privacy in Canada*

2. *Initiatives to Protect Privacy*

III. *The Act: The Government's Answer to Concerns about the Collection of Personal Information*

IV. *The Act: Responsive to the Interests of the Business Community*

1. *The Close Relationship Between Business and Government*

2. *The Consumerization of Citizenship*

3. *The Effects of Consumerism on Governmental Decision-making*

4. *The Protection of Human Rights: Lost in the Commodity Shuffle*

5. *The Process of Legitimizing the Legislation: Sugar-Coating Bad Medicine*

V. *Recommendations and Conclusions*

1. *The Charter of Rights and Freedoms*

2. *The Privacy Charter*

3. *Improving the Act*

Appendix A

Appendix B

Introduction

The *Personal Information Protection and Electronic Documents Act*[2] is the federal government's most recent legislative effort to protect the privacy of Canadians. It was inspired by the increased need for privacy protection due to the proliferation and commercial importance of Canadians' personal information. The Act was promulgated as a result of the inadequacy of the current privacy regime in Canada to protect personal information in the private sector. In this paper, I will highlight the legal (particularly human rights) problems faced by the proliferation of personal information, outline current Canadian legislation to protect privacy and then discuss how the Act attempts to fill the gaps in privacy protection.

I hope to demonstrate that the Act fails to achieve its declared goal of protecting privacy. First, I will argue that the alignment of the interests of government and the self-interest of business groups leads to legislation that protects the short-term needs of business stakeholders instead of long-term policy statements that promote the public good. Next, I contend that the government justifies its narrow, market-focused goals by constructing citizens as consumers with market needs instead of human rights. I will then demonstrate, through a comparative analysis of the Act, the Privacy Charter proposed by the House of Commons Standing Committee on Human Rights and the Australian Privacy Charter, the extent to which the Act fails to achieve its stated purpose of protecting Canadians' right to privacy. I posit that the Act is made acceptable to Canadians by the urgently felt need to address the issues created by the inevitable and relentless evolution of technology. Finally, I propose solutions that may improve the protection of privacy in Canada.

---

2. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [passed as the Act, assented to April 13, 2000, hereinafter the "Act"].

I. *The Collection of Personal Information in Canada*

1. *How Personal Information is Collected*

Personal information is collected by both the public and private sector. In particular, the government collects information from answers supplied by citizens in order to receive government services. These may include government grants (Human Resources Development Canada) or Employment Insurance,[3] censuses (through StatsCan[4]), through the enforcement of the law,[5] property assessments, customs declarations and information provided to Revenue Canada in tax returns[6] or to Elections Canada by voting lists.[7]

The primary private sector collectors of personal information are banking institutions, insurance and credit card companies, private-sector health care providers like pharmacies, telecommunications and cable companies, chartered accountants, and corporations involved in direct marketing.[8] The private sector also acquires personal information through an array of media, including surveys, the exchange of personal information for free services or products,[9] billing records, customer and subscriber

---

3. For example, the federal government has cross-matched information provided to Human Resources Development Canada and Revenue Canada to determine how many of those people who obtained grants from HRDC continue to remain self-supporting. House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, "Privacy: Where Do We Draw the Line", online: The Canadian Parliament <http://www.parl.gc.ca/committees352/huso/reports/03_1997-04/cove.html> (date accessed: 10 May 2001) [hereinafter "Standing Committee"].
On May 29, 2000 the federal government announced that, in response to concerns voiced by the Privacy Commissioner and citizens, it was dismantling the Human Resources Development database on Canadian citizens, online: Human Resources Development Canada <http://www.hrdc-drhc.gc.ca/common/news/dept/00-39.shtml> (last modified: 15 March 2001).
4. For more information see online: StatsCan <http://www.statcan.ca/english/services/> (last modified: 1 May 2001).
5. "Privacy: The protection of personal information", online: Strategis <http://ecom.ic.gc.ca/english/privacy/632d13.html> (last modified: 12 December 2000).
6. For example, online: Canada Customs and Revenue Agency <http://www.ccra-adrc.gc.ca/eservices/strategy/> (date accessed: 10 May 2001).
7. For more information see online: < http://www.elections.ca/home.asp?textonly=false> (last modified: 6 April 2001).
8. Information obtained generally from: V. Steeves, "We Need More Protection From Invasion of Privacy", online: Human Rights Research and Education Centre, University of Ottawa <http://www.uottawa.ca/hrrec/techno/citizen.html> (date accessed: 12 May 2001); *supra* note 5; "What is privacy?", online: Strategis <http://ecom.ic.gc.ca/english/privacy/632d4.html> (last modified: 10 December 2001).
9. M. Stroh, "Privacy and the Net: Where is it heading? Web sites can follow a trail with your data, recording every move" *The Ottawa Citizen* (3 January 2000), online: Human Rights Research and Education Centre, University of Ottawa <http://www.uottawa.ca/hrrec/techno/techno.html> (last modified: 4 December 1997).

mailing lists and through exchanging or buying compiled information.[10] On the Internet, information is commonly obtained through tracking individuals' activities on-line using "cookies"[11] or by collecting "click-stream data"[12] of pages visited and downloaded.

2. *What Type of Personal Information is Sought?*

Personal information is collected from Canadians as they engage in all aspects of civic and consumer life. At the most basic level the type of data sought is demographic, such as name, address, e-mail address, age, marital status, sex and social insurance number. This basic information is then supplemented by information particular to the projected end-use of the information sought.[13]

The attitudes, opinions and beliefs of individuals are valuable personal information, as are the contents of personal phone, fax and e-mail communications.[14] Medical information, in particular on drugs prescribed, allergies and medical treatment received, is collected. Also biological and biometric data is compiled such as genetic information, finger scans, fingerprints, hand geometry and retinal scans.[15]

Geographical information may be sought such as place of residence (including type of residence and neighbourhood), location at any given time, times of entry and exit into particular structures or facilities (*e.g.* subways, parking lots or toll highways).[16] Law enforcement information may be collected which includes criminal records, warrants or civil judgments. Financial information may be gathered such as debt or credit information, loans, repayments, savings, withdrawals, deposits and use

---

10. H.J. Smith, *Managing Privacy* (Chapel Hill: University of North Carolina Press, 1994) [hereinafter "Managing Privacy"].

11. Cookies are text files stored on a user's hard-drive with an identification number and other information which allows Web operators to easily identify a particular user on-line (*supra* note 9). Information is also collected on-line through newsgroups, e-mail and chat sessions (J. Rothchild, "Protecting the Digital Consumer: The Limits of Cyberspace Utopianism" (1999) 74 Ind. L.J. 893).

12. 1998-1999 Annual Report of the Privacy Commissioner, online: Office of the Privacy Commissioner <http://www.privcom.gc.ca/ar/02_04_07_e.asp> (date accessed: 13 May 2001) [hereinafter "1999 Annual Report"].

13. There is unlimited scope for the collection of personal information and I do not intend to provide a comprehensive survey of all personal information collected.

14. G. Walters, "Digitizing Technology, Transforming Ourselves" (1999) 10 N.J.C.L. 373 at 379 [hereinafter "Transforming Ourselves"].

15. *Ibid.*

16. Transforming Ourselves, *supra* note 14 at 375. See also S. Garfinkel, "Privacy and the New Technology: What They Do Know Can Hurt You", online: The Nation <http://past.thenation.com/cgi-bin/framizer.cgi?url=http://past.thenation.com/issue/000228/0228garfinkel.shtml> (date accessed: 13 May 2001).

of particular services.[17] Most popular is the compilation of consumer information, such as the amount and type of good purchased, frequency of purchases, patterns of purchases and use made of consumer products.[18]

3. *The Purposes of Collecting Personal Information*

Personal information can be collected for the sole purpose of ensuring that the information is available if needed (this is referred to as data warehousing). However, personal information can also be compiled, manipulated and transformed through combining information within the collecting organization or by merging information from separate collections and organizations. The consolidation of data has been facilitated by the increased computerization of information and has been encouraged through technologies such as relational computer software (for grouping and cross-referencing data), sophisticated linear searching programs[19] and Artificial Intelligence (AI)[20] that make the processing of information cheap and convenient.[21] Raw or compiled data can then be resold for profit.[22] The two major end-uses for personal information are targeted marketing and the minimization of risk.

Targeted marketing uses data compiled as demographic or psychographic profiles.[23] These profiles (which can identify both consumer preferences and where to find those consumers[24]) are then used to directly

---

17. I. Lawson, *Privacy and Free Enterprise* (Ottawa: Public Interest Advocacy Centre, 1992) at 17 [hereinafter "Free Enterprise"].
18. 1995-1996 Annual Report of the Privacy Commissioner, online: Office of the Privacy Commissioner <http://www.privcom.gc.ca/ar/02_04_04_e.asp> (date accessed: 13 May 2001).
19. Managing Privacy, *supra* note 10 at 7.
20. Artificial intelligence, in particular, can be used to scan databases and detect patterns and relationships between data contained within the database (D. Banisar, "Big Brother Goes High-Tech", online: Media Awareness Network <http://www.media-awareness.ca/eng/issues/priv/resource/brother.html> (date accessed: 13 May 2001)).
21. Free Enterprise, *supra* note 17 at 4.
22. *Supra* note 9. See also online: Undercurrents <http://www.tv.cbc.ca/undercurrents/> (date accessed: 13 May 2001).
23. A psychographic profile attempts to classify individuals into groups according to their attitudes, interests and opinions as opposed to strict demographic criteria like age, residence and occupation. To achieve this cataloguing, psychographics asks normal and then obscure questions such as: Could you skin a dead animal? Would you vote for a communist to be mayor of your city? The primary distinction between demographic and psychographic profiles is that demographic profiles are based on facts (such as age, sex, occupation) whereas psychographic profiles are based on feelings. For example, if women of an identical demographic buy different types of cars then this difference is explained by psychographics (Managing Privacy, *supra* note 10 at 77).
24. The Privacy Commissioner outlined in his most recent report the useful marketing finding that men who go to buy diapers in the evening usually buy beer on their way home (1999 Annual Report, *supra* note 12).

target individuals, in contrast to traditional marketing methods which indiscriminately advertise to a general public.[25]

The second major use of personal information entails exchanging and matching information between organizations to minimize institutional risk. Banks and credit granting institutions use personal information (about income and credit rating, for example) to gauge the level of lending risk that a prospective client presents. Insurance companies use compiled personal information (about health or lifestyle, for example) to make decisions about whether or at what rate to insure an individual.[26] Personal information may also be used in decisions about whom to hire.[27]

4. *Concerns Over the Collection of Personal Information*

The collection, compilation and exchange of information have raised concerns among those whose information is collected. First, citizens are concerned that their information is being used for purposes other than those for which it was collected.[28] Second, there are worries that the public and private sectors are collecting more information than is required, often under false pretenses, without obtaining meaningful consent.[29]

---

25. Managing Privacy, *supra* note 10 at 8. Common examples of targeted micromarketing are the use of credit card purchase records to directly target promotional offers for such things as travel, recreation and automobile purchases or the creation of purchasing circles and or recommended purchasing lists by bookstores (*i.e.* Amazon.com) (*supra* note 9). Further examples are outlined in Senate, Standing Committee on Social Affairs, Science and Technology, Evidence, issue 2 (29 Nov. 1999), submissions of Phillipa Lawson at 10 [hereinafter "Issue 2"], where she states:

> [a] Montreal woman [had] been diagnosed with cancer. No sooner did she get home from the hospital than she received a telephone solicitation from a funeral home. New mothers who give birth at hospitals are frequently inundated with the marketing of baby products. While this may seem harmless, it is not appreciated when the baby has died. In one reported case, a man who had consulted a medical clinic for sexual dysfunction later received direct mail advertising cures for impotence.

26. V. Steeves, "A Better Road Map for the Information Highway: Critical Human Rights Issues in the Access and Privacy Field", online: Human Rights Research Centre, University of Ottawa <http://www.uottawa.ca/hrrec/publicat/mbs.html> (date accessed: 13 May 2001) [hereinafter "Road Map"].

27. See also Issue 2, *supra* note 25: "A recent survey of Fortune 500 companies indicated that over half admitted to using medical information in employment decisions, often without the individual's knowledge or consent."

28. A recent example is the matching of returning traveler's customs declarations with their employment insurance claims to detect potential abuse of EI (1999 Annual report, *supra* note 12).

29. In the public sector, 20% of the Canadian population every five years is required to fill out the long form census which requires such information as the mortgage payments, brands of products used and religion (*supra* note 22). In the private sector, marketing surveys are frequently disguised as contests or games. For example, U.S. car dealerships often have a computer where a potential car buyer enters information to help the computer match a car to their personality type. A car is then recommended to the customer while a second result is then printed in the dealership's offices recommending the type of sales strategy to use on the customer such as "hard-sell" or "friendly sell". (Managing Privacy, *supra* note 10 at 99).

Thirdly, there is no mechanism for ensuring that personal information is eventually deleted[30] and there are few means to establish what information actually exists about oneself.[31] Citizens are also concerned that their personal information is being shared with people whose access was not contemplated in their original consent.[32]

Further, data collectors may be coercing citizens by tying personal information to access to services or even to threats of prosecution.[33] Personal data that is erroneous can proliferate (through matching and exchanging of databases) and can result in the denial of services, particularly if no means exist to correct the data.[34] Additionally, if information is combined then its sum may be more than its parts and can result in a highly accurate and detailed profile of an individual consumer.[35] Finally, access by decision makers to large pools of personal data may reduce individual judgment capability and result in a quantitative and formulaic process decision making process.[36]

30 *Supra* note 8 at 4.

31 *Supra* note 5 at 4.

32 This concern is particularly pronounced regarding the use of information collected by government that is then sold for marketing purposes (*supra* note 8). Another example, outlined by the Privacy Commissioner, is that anytime a transaction is completed using an Air Miles card, information about that transaction is packaged and shared with 134 corporate sponsors of Air Miles (1999 Annual Report, *supra* note 12).

33 For example, failing to complete a federal government census may result in a fine or imprisonment (*supra* note 22). As well, employees may be required to undergo a genetic or drug test to ensure they get or keep a job (Standing Committee, *supra* note 3 at 6).

34 An example is an incorrect credit history which is then used to deny a bank loan. (Managing Privacy, *supra* note 10 at 116-117).

35 For example, in an anonymous study, Bank A admitted to buying anonymous data from an outside vendor. Bank A would exchange information such as names and addresses and in return receive the following information directly correlated to those names and addresses:

1. *Purchasing Power Data:* the individual's purchasing power, use of credit accounts and the type of credit, the degree to which the individual is willing to commit to fixed payment obligations and estimated household income.
2. *Purchasing Activity Data:* A measure of a person's propensity to use bank cards, travel cards, retail cards, oil and auto cards and their total number of active credit accounts.
3. *Consumer Shopping Data:* the consumer categorized by shopping preferences (cash shopper, prestige shopper, value shopper, price shopper, etc.).
4. *Demographic Data:* date of birth, marital status, gender and classification into one of sixty-four market segments based on financial and geodemographic data.

Managing Privacy, *ibid.* at 114.

36. An example of this concern includes the large number of credit cards issued annually to animals or the deceased (Managing Privacy, *ibid.* at 122).

II. *The Underlying Privacy Protection Framework*

The apprehension among citizens about the collection of personal information is manifested in increased concern about violations of personal privacy which has been demonstrated in surveys and opinion polls,[37] complaints to the Office of the Privacy Commissioner,[38] and other initiatives such as websites, group action, seminars, studies and workshops.[39] The criticism focuses on the perceived inadequacies of the legislative and common law protection of privacy.

---

37. The results of some of these surveys are outlined below:

> Public surveys of Canadians have consistently revealed a remarkably high level of concern over the issue of privacy. The 1992 Canadian Privacy Survey by Ekos Research Associates Inc. found that *92 percent of the 3 000 Canadians interviewed believed privacy to be an important issue, and that 60 percent believed they have less personal privacy now than a decade ago...* A 1994 Gallup Canada survey for Andersen Consulting revealed that over *80 percent of the Canadians polled expressed concern* about the personal information about them that might be collected by companies through the information highway. These studies suggest a pervasive belief that personal privacy is under siege from a range of technological, commercial and social threats and that something must be done about it. [emphasis added]
>
> Communications Development and Planning Branch Spectrum, Industry Canada, "Privacy and the Canadian Information Highway, Building Canada's Information and Communications Infrastructure", online: Strategis <http://ecom.ic.gc.ca/english/privacy> (date accessed: 27 March 2000).

More recently (in 1998) a study by Ekos found that "94 per cent of Canadians believe it is increasingly important to have safeguards for personal information on the Internet. Canadians, moreover, are becoming much more knowledgeable about privacy issues." (Senate, Standing Committee on Social Affairs, Science and Technology, Evidence, issue 5 (2 Dec. 1999).)

38. As the Privacy Commissioner documents in his 1998-1999 report: "Incoming complaints jumped past the 3000 mark for the first time in the office's history—new complaints reached 3105 for the 1998-99 fiscal year." (1999 Annual Report, *supra* note 12)

39. A study conducted by the House of Commons Standing Committee on Human Rights concludes that:

> [W]e could not but be amazed by the degree of consensus that emerged in each of our meetings... *they [citizens] all believe that privacy matters* [emphasis added].

Standing Committee, *supra* note 3.

1. *The Legal Protection of Privacy in Canada*

Canada is committed internationally to the protection of privacy generally by art. 12 of the *Universal Declaration of Human Rights* which provides that:

> No one shall be subjected to arbitrary interference with his privacy, 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.[40]

Article 12, however, has not been directly implemented in Canadian law. The European Union enacted the *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*[41] in 1995 to harmonize data protection within the European Union. It compels European states to enact legislation to protect personal information in their public and private sectors. It also requires that states wishing to exchange information with European Union member nations have an "adequate level of protection", otherwise those transfers will be blocked. Although the Directive does not protect data collected from Canadians in Canada, it has motivated Canadian legislators to enact legislation to protect data, as inadequate Canadian data protection laws could be a significant non-tariff trade barrier between Canada and the European Union.[42]

Domestically, the highest legal authority for a right of privacy is the *Canadian Charter of Rights and Freedoms*[43] which, while not explicitly providing protection of privacy, has been interpreted to protect dignity,

---

40. A provision similar to art. 12 is contained in art. 17 of the *International Covenant on Civil and Political Rights*, 19 December 1966, 999 U.N.T.S. 171, art. 2, Can. T.S. 1976 No. 47, 6 I.L.M. 368 (entered into force 23 March 1976, accession by Canada 19 May 1976).
41. *Official Journal of the European Community* November 23, 1995, no. L281 at 31.
42. *Supra* note 8.
43. Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [hereinafter *Charter*].

autonomy and privacy in sections 7,[44] 8[45] and 2(b).[46] In particular, s. 8 of the *Charter* has been interpreted by the Supreme Court of Canada to address violations of privacy caused by electronic surveillance and the use of personal information stored on databases.[47] However, the *Charter* is an inherently limited means for protecting privacy as it directly applies only to activities involving a government actor (not the private sector) and infringements can be justified under section 1 as reasonable limitations in a free and democratic society.

---

44. Section 7 provides that "Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice." This provision implements art. 3 of the *Universal Declaration of Human Rights* which provides: "Everyone has the right to life, liberty and security of the person."

Section 7 liberty interests have been held to encompass not only physical liberty, but also fundamental concepts of human dignity, individual autonomy and privacy (*R.* v. *Morgentaler* [1988] 1 S.C.R. 30) and *R.* v. *Jones* ([1986] 2 S.C.R. 284)). In *B.(R.)* v. *Children's Aid Society of Metropolitan Toronto* [1995] 1 S.C.R. 315 the court did not contest the notion that s. 7 rights relate not only to physical constraints on liberty, but may extend to a sphere of personal autonomy that the state is precluded from invading. Finally the autonomy interest of choosing where one lives is protected by s. 7 (*Godbout* c. *Longueuil (Ville)*, [1997] 3 S.C.R. 844).

See generally: A.W. MacKay, "The Waves of Information Technology, the Ebbing of Privacy, and the Threat to Human Rights" (1999) 10 N.J.C.L. 411. [hereinafter "Ebbing"]

45. Section 8 provides that: "Everyone has the right to be secure against unreasonable search or seizure."

Section 8 has been interpreted by the Supreme Court of Canada as applying outside of the criminal context (*R.* v. *Edwards*, [1996] 1 S.C.R. 128) and is a personal right (*R.* v. *Plant*, [1993] 3 S.C.R. 281) that protects an individual's reasonable expectations of privacy (*Hunter* v. *Southam Inc.*, [1984] 2 S.C.R. 145). The expectation of privacy can depend on: one's status (there is a lower expectation of privacy if one is in police custody (*R.* v. *Stillman*, [1997] 1 S.C.R. 607)), one's social class (a student has a lower expectation of privacy than others (*R.* v. *M.(M.R.)*, [1998] 3 S.C.R. 393)), and the location of the privacy violation (for example, there is a lower expectation of privacy in a school (*R.* v. *M.(M.R.)*).

46. Section 2(b) holds that:

> Everyone has the following fundamental freedoms:...
> (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication.

In *R.* v. *Sharpe*, [1999] B.C.J. No. 1555 the British Columbia Court of Appeal found that s. 163.1(4), which prohibits the possession of child pornography in a wide array of circumstances, violated the defendant's s. 2(b) rights to freedom of expression as it impinged on the value of liberty, autonomy and privacy protected by the *Charter*. See also *R.* v. *Keegstra*, [1990] 3 S.C.R. 697 which upheld the constitutionality of s. 319(2) of the Criminal Code as it specifically excluded private conversations, thus protecting individual privacy (Ebbing, *supra* note 44).

47. The court has been reluctant to extend s. 8 protection to personal information stored in databases (*R.* v. *Plant*, *supra* note 45), but has interpreted s. 8 to protect against electronic surveillance in the criminal context (*R.* v. *Duarte*, [1990] 1 S.C.R. 30 and *R.* v. *Wong*, [1990] 3 S.C.R. 36). The level of constitutional protection afforded personal information may be limited by the relaxed application of s. 8 to administrative law (*R.* v. *McKinlay Transport Ltd.*, [1990] 1 S.C.R. 627).

In Quebec, art. 5 of the *Quebec Charter of Human Rights and Freedoms*[48] protects the right to privacy by guaranteeing every person the right to respect for his or her private life and providing for a right to compensation if that right is infringed. This document enjoys quasi-constitutional status as it prevails over all other enactments in the province unless there is express wording to the contrary.[49]

Both federal and provincial governments have enacted legislation to protect the collection and exchange of personal information in the public sector. The federal government enacted the *Privacy Act* in 1982 as a means of controlling the collection, use and disclosure of personal information about federal government employees and those who use its services. It applies to all federal government institutions.[50] The legislation also established the Office of the Privacy Commissioner whose role is to monitor and resolve disputes under the *Privacy Act*. Most provinces have enacted similar legislation that applies to their provincial public sectors.[51] However, no province other than Quebec has legislation governing the use and exchange of personal information by the private sector. The Quebec legislation, *An Act Respecting the Protection of Personal Information in the Private Sector*,[52] is discussed below in s. 6.

The common law has begun to recognize a tort of invasion of privacy[53] and four provinces, British Columbia,[54] Manitoba,[55] Saskatchewan[56] and Newfoundland,[57] have enacted legislation that creates tortious liability

48. R.S.Q., c. C-12.

49. Standing Committee, *supra* note 3 at 17.

50. "All federal departments, most federal agencies and some federal Crown corporations" comprise "federal institutions." The information protected by the *Privacy Act* includes name, address, race, age, ethnicity, financial status, employment history, criminal records, medical history and personal views. Specific categories of personal information held by government are more fully protected by the *Income Tax Act* and the *Statistics Act* (D.C. Kratchanov, *Personal Information and the Protection of Privacy, Appendix M to the Proceedings of the 1995 Meeting of The Uniform Law Conference of Canada*, online: Uniform Law Conference of Canada <http://www.law.ualberta.ca/alri/ulc/95pro/e95m.htm> (date accessed: 13 May 2001) [hereinafter "ULCC"]).

51. The provinces that have enacted legislation are Quebec, Ontario, Saskatchewan, British Columbia, Alberta, Nova Scotia and the Yukon.

52. R.S.Q., c. P-39.1 [hereinafter the "Quebec Act"].

53. For more information see A.M Linden & L.N. Klar, *Canadian Tort Law* (Markham: Butterworths, 1994) at 93. The common law protection of privacy may also include the tort of appropriation of personality (*Krouse* v. *Chrysler Canada Ltd.* (1974), 40 D.L.R. (3d) 15 (Ont. C.A.)).

54. *Privacy Act,* R.S.B.C. 1996, c. 373.

55. *Privacy Act*, R.S.M. 1987, c. P-125.

56. *Privacy Act*, R.S.S. 1978, c. P-24.

57. *Privacy Act*, R.S.N. 1990, c. P-22.

for the invasion of privacy. However, these provisions have not been the subject of intensive judicial consideration and have not acted as a potent means for protecting privacy.[58]

Thus, while some legally enforceable protection of privacy and personal information exists in Canada it is either limited to the public sector, contained within voluntary private sector or professional codes or relies on individual enforcement through civil actions. Except in Quebec, there is no constitutional or legislative commitment to protect a broad right of privacy.

2. *Initiatives to Protect Privacy*

Solutions have been proposed to remedy the inadequacies caused by limited legal protection of privacy and personal information in Canada, particularly with regard to the private sector. Two are worthy of mention. First, the Standing Committee on Human Rights has proposed a *Canadian Charter of Privacy Rights* (Privacy Charter) to declare and entrench rights to privacy.[59] (See Appendix A.) This charter may even be enacted into law if it is passed by the Legislature.[60] The Privacy Charter is closely modeled after the *Australian Privacy Charter*, a non-binding policy document developed by the Australian Privacy Charter Council.[61] (See Appendix B.) It has also been suggested that a right to privacy be included

---

58. ULCC, *supra* note 50.

59. The Standing Committee of the House of Commons on Human Rights and the Status of Persons with Disabilities spent 10 months exploring privacy rights and the new technologies. The research process involved discussions with a wide cross-section of citizens across Canadian constituencies in a townhall discussion format. The Committee of Members of Parliament wrote a final report recommending the government enact a Privacy Charter. V. Steeves, "A Response to Professor Walter's Article, 'Digitizing Technology, Transforming Ourselves'" (1999) 10 N.J.C.L. 445 at 451. [hereinafter "Response"]

60. Bill S-27: *An Act to guarantee the human right of privacy* was introduced by Senator Sheila Finestone and passed first reading on June 15, 2000. It was then re-introduced and passed first reading on March 13, 2001 as Bill S-21 and was sent to the Social Affairs, Science and Technology Committee on April 26, 2001, online: The Canadian Parliament <http://www.parl.gc.ca/37/1/parlbus/chambus/senate/deb-e/prog-e.htm> (date accessed: 6 May 2001).

61. The Australian Privacy Charter was developed in 1992 by a group of 25 invited members and has received significant attention in Australia and abroad. The aim of the principles is to act

> as a general statement of the privacy protection that Australians should expect to see observed by both the public and private sectors. They are intended to act as a benchmark against which the practices of business and government, and the adequacy of legislation and codes, may be measured. They inform Australians of the privacy rights they are entitled to expect and should observe.

For more information see: Australian Privacy Charter Council <http://www.anu.edu.au/people/Roger.Clarke/DV/PrivChHist.html> (date accessed: 13 May 2001).

in the *Canadian Charter of Rights and Freedoms*.[62] The advantages and disadvantages of each option will be discussed in the Recommendations (section V).

III. *The Act: The Government's Answer to Concerns about the Collection of Personal Information*[63]

The federal government's response to Canadians' concerns about the security and privacy of their personal information was to pass the Act.[64] Responsibility for its creation lay with Industry Canada.[65]

Briefly, the Act applies to personal information[66] collected, used or disclosed by the federally regulated private sector (*e.g.* interprovincial transportation, banking, telecommunications and broadcasting) and by federal government entities not covered by the federal *Privacy Act*.[67] It also applies to information that is exchanged or transferred inter-provincially and internationally. After three years, the Act will apply to

---

62. *Supra* note 5 at 5. Recommendation by the B.C. Freedom of Information and Privacy Association, Canada's Coalition for Public Information, Privacy Partners, and the Public Interest Advocacy Centre. For more support see D. Gutstein, *E.con: How the Internet Undermines Democracy* (Toronto: Stoddart, 1999) at 285 [hereinafter "E.con"] and the Standing Committee, *supra* note 3 at 17. Note as well that the Uniform Law Conference of Canada has proposed a *Uniform Electronic Commerce Act*. However, this proposed Act addresses the legal issues of electronic commerce (contract formation and technicalities of the sale of goods) rather than substantive issues of privacy (ULCC, *supra* note 50).

63. For the purposes of this paper I will only be discussing Part I of the Act. Part II legislates with respect to electronic documents and is regarded by many as a separate piece of legislation even though it has been enacted as part of the Act (Standing Senate Committee on Social Affairs, Science and Technology, Issue 4 – Evidence, Ottawa, Monday, December 1, 1999).

64. *Supra* note 2. In the words of Industry Canada: "The purpose of the *Personal Information Protection and Electronic Documents Act* is to provide Canadians with *a right of privacy* with respect to their personal information that is collected used or disclosed by an organization in the private sector . . . . " [emphasis added] ("Backgrounder Privacy Provisions Highlights", online: Strategis <http://ecom.ic.gc.ca/english/fastfacts/43d8.html> (date accessed: 13 May 2001).

65. The longer title of the Act states that it is:

> *An Act to support and promote electronic commerce* by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act [emphasis added]. (*Supra* note 2.)

66. Personal information is defined in s. 2 as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." *Ibid.*

67. *Ibid.*, s. 4(2).

personal information collected, used, or disclosed by both the federal and provincial public sector and the private sector.[68]

The Act enacts substantive privacy provisions as Schedule I. However, these provisions are only recommendations and are *not* legally binding obligations.[69] Schedule I is based on the Canadian Standards Association's *Model Code for the Protection of Personal Information.*[70] It attempts to address some of the concerns I outlined in Section I,4. Principle 4.2 requires that the purpose for which data are used be identified by the organization and that the organization be prepared to explain this purpose to individuals. As well, knowledge and consent are required for the collection, use and disclosure of personal information[71] and organizations are advised to be open about their data management policies.[72]

Principle 4.4 confronts problems of over-collection of data by requiring that collection of information be limited to information necessary to fulfill the purposes identified in Principle 4.2. Additionally, the Schedule stipulates that information cannot be obtained through deception.[73]

The purpose of Principle 5 is to allay concerns about indefinite retention of personal information; it requires that information be retained only for as long as it is required and then it should be destroyed, erased or made anonymous.[74]

By requiring that consent be given to the use of personal information for new purposes, the Act addresses fears that personal information might be disseminated without the knowledge of the individual.[75] Organizations are also required to protect data (based on its level of sensitivity) from loss, theft or unauthorized modification.[76] This principle attempts to control who has access to personal information. The Schedule recommends that individuals should be given access to their personal information[77] and organizations must be open to the public about their policies and

---

68. *Ibid.*, s. 30. Note that the Act does not apply to individuals who collect information for personal or domestic use (s. 4(2)(b)) and does not apply to organizations collecting information for journalistic, artistic or literary purposes (s. 4(2)(c)). Provinces can remove themselves from the application of the Act by enacting legislation that is substantively similar to the Act's provisions.
69. *Ibid.*, s. 5(2).
70. *Supra* note 64.
71. *Supra* note 2, Sch. I, principle 4.3.
72. *Ibid.*, principle 4.8.
73. *Ibid.*, principle 4.3.5.
74. *Ibid.*, principle 4.5.3.
75. *Ibid.*, principle 4.2.4.
76. *Ibid.*, principle 4.7.
77. *Ibid.*, principle 4.9.
78. *Ibid.*, principle 4.8.

practices regarding the management of personal information.[78] These provisions aid in determining what information actually exists about oneself and limiting its use.

The correctness of data is dealt with by Principle 4.6, which requires that personal information be "accurate, complete and up-to-date." The Schedule recommends that the organization correct information if an individual demonstrates that it is incorrect.[79]

The web of responsibility is widened by the recommendation that organizations are accountable for personal information in their control or transmitted to third parties.[80] Enforcement of the principles is also encouraged by Principle 4.10 which recommends that individuals be allowed to challenge an organization's compliance with the recommendations of the Schedule.

The Act does not address the concern that the provision of goods and services may be tied to divulging personal information. Nor are there any general statements of policy in the Act restricting the creation of highly detailed individual profiles or discouraging mechanical decision making based on database information.

Enforcement of the provisions of the Act lies with the federal Privacy Commissioner, who can investigate complaints, report on those complaints and attempt to resolve disputes.[81] The Commissioner can also independently initiate audits.[82] Should a claim remain unresolved, a complainant or the Commissioner can apply to the Federal Court for a hearing where the court can order an organization to "correct its practices" and publish notice of any action taken to correct its practices; the court can also order damages (including punitive damages).[83] The Commissioner is generally responsible for developing information programs "to foster public understanding, and recognition of the purposes" of the Act and for undertaking and publishing research about the protection of personal information. The Commissioner must also encourage organizations to develop policies and practices that comply with the principles of the Schedule.[84]

An evaluation of the substantive provisions of the Act as well as its omissions will follow in the subsequent sections of this paper. The analysis will highlight both the weakness of the substantive provisions

---

79. *Ibid.*, principle 4.9.5.
80. *Ibid.*, principle 4.1.
81. *Ibid.*, see Division 2, "Remedies."
82. *Ibid.*, Division 3, "Audits."
83. *Ibid.*, ss. 14-16.
84. *Ibid.*, s. 24.

and the significance of the omissions and tie those to larger trends in governance, citizenship and consumerism.

IV. *The Act: Responsive to the Interests of the Business Community*

Regardless of the assertions of the federal government,[85] the Act was not passed as substantive privacy protection legislation. Instead its purpose is to facilitate e-commerce by reassuring Canadians that their personal information may be protected. This will be demonstrated by outlining first, the growing convergence of business and government decision-making and the subsequent construction of the Canadian citizen as the Canadian consumer. It will then be shown that the "consumerization of citizenship" and the fragmentation of social interaction through the commodification of information have resulted in short-sighted legislative efforts (*i.e.* the Act) to protect data not human rights. Finally, I will demonstrate how the Act is made more palatable to Canadians through the spread of doctrines of technological determinism and inevitability.

1. *The Close Relationship Between Business and Government*

A close relationship between business and government may result in corporate-style governance. Legitimate democratic governance requires the exercise of power by individual citizens. Corporatism, however, relies on the exercise of power primarily by groups.[86] These groups can be corporations, but also include other entities such as consumer organizations, think tanks or lobbying associations. Corporatism functions within the structures of democracy. However, its ends are fundamentally undemocratic.

True democracy achieves legitimacy by substantiating its citizens' rights through acting in the public good since "[g]overnment is the only

85. See the comments of Industry Canada, *supra* note 64.
86. J.R. Saul, *The Unconscious Civilization* (Concord, Ont.: House of Anansi Press, 1995) at 62.
87. *Ibid.* at 29.

organized mechanism that makes possible that level of shared disinterest known as the public good."[87] Corporatism, on the other hand, promotes the self-interest of groups over the public good;[88] the role of self-interest is masked by referring to citizens as public interest groups.[89] Decisions in a corporatist society are made by the groups that are its constituency in the form of group negotiations, 'multistakeholder' or consensual alliances.[90]

Citizens are "represented" and can "participate" in the decision making process through consumer or public interest groups. Through direct consultations, the citizen's voice can be 'heard' as a factor to consider in the decision making process. However, this voice is ignored as the important decisions have already been made elsewhere[91] by government and business interest groups in informal private governments[92] that

---

88. *Ibid.* at 76. Ursula Franklin has discussed the shift of government from fulfilling the interests of the public good (referred to as indivisible benefits) to satisfying self-interest (named as divisible benefits) in the specific context of technological development in Canada. Divisible benefits accrue when five people, for example, plant tomatoes and then those same five people share those tomatoes once they have grown. Indivisible benefits, however, accrue to those who may not have made sacrifices. For example, if one actively campaigns to reduce pollution then benefits accrue to both yourself and your neighbours who did nothing. As she states:

> Technology has changed this notion about the obligations of a government to its citizens [to provide indivisible benefits]. The public infrastructures that made the development and spread of technology possible have become more and more frequently roads to divisible benefits. Thus the public purse has provided the wherewithal from which the private sector derives the divisible benefits, while at the same time the realm from which the indivisible benefits are derived has deteriorated and often remains unprotected.

U. Franklin, *The Real World of Technology* (Concord, Ont.: House of Anansi Press, 1999) at 66.

89. An example of this is provided by Industry Canada when commenting on the CSA Standard: "First, it represents a consensus among key stakeholders from the private sector, *consumer and other public interest organizations*, and some government bodies." [emphasis added] (Industry Canada, "Privacy: The protection of personal information", online: Strategis <http://ecom.ic.gc.ca/english/privacy/632d5.html> (date accessed: 13 May 2001)).

90. *Supra* note 86.

91. As Saul states:

> Not surprisingly, both the referendum and direct democracy are a happy marriage with corporatism. The complex, real questions are dealt with behind the scenes through efficient "interest mediation" between the different interest groups. As for the citizenry, they are occupied and distracted by the fireworks of their direct involvement on the big questions and their direct relationship with the big people.
>
> *Ibid.* at 109.

92. E.con, *supra* note 62 at 75. These informal private governments are composed of "federal and provincial government agencies, corporate pressure groups, major corporations, members of the media, (rarely) public-interest pressure groups, and other who attempted over a long period of time to influence policy in a particular field."

produce an elite consensus.[93] Therefore, instead of attempting to fulfill its commitment to the public good, government seeks to balance the interests of citizens with the democratically *irrelevant* needs of non-citizens (corporations).

The use of negotiation, consensus and direct consultation portray corporatist governance as *more* populist and representative than legitimate democracy.[94] Comments by Professor Errol Mendes, Director of the

---

93. A strong current of academic thought holds that the corporate/governing elite in a country is more closely allied with the governing elite of other countries and transnational corporations, than with the citizens they represent. (R. Babe, *Communication and the Transformation of Economics: Essays in Information, Public Policy, and Political Economy* (Boulder: Westview Press, 1995) at 207 [hereinafter "Babe"]) See also: M. Dobbin, *The Myth of the Good Corporate Citizen: Democracy Under the Rule of Big Business* (Toronto: Stoddart, 1998) at 5.
An example of the close identification with international interests is provided in an Industry Canada document: "[The Act] should include a blend of voluntary and regulatory approaches and, given the global reach of electronic commerce, should be consistent with approaches to consumer protection *agreed to by the international community.*" (Industry Canada, "Principles of Consumer Protection for Electronic Commerce", online: Strategis <http://strategis.ic.gc.ca/SSG/ca01185e.html> (publication date: 8 November 1999)).
As well, the Canadian government has placed much of its decision-making on foreign policy in the hands of "Team Canada."

> As Robert Babe comments:
>
> The idea that "Team Canada" is forming policies, such as free trade and information highway initiatives, makes a lot of sense once it is realized... that the beneficiaries of such initiatives are predominantly "Team Canada's" transnational corporate members.

Babe, *ibid.* at 203.
Finally, Industry Canada also admits to seeking an elite consensus: "to strengthen Canada's voice and impact on issues of network and device interoperability, the federal government should seek a stronger, more cooperative set of arrangements with Canadian Industry to put forward Canadian positions to international standards bodies." (Industry Canada, Chapter 2: Building Canada's Information Infrastructure, Strategis online: <http://strategis.ic.gc.ca./SSG/ih01640e.html> (publication date: 8 October 1997) [hereinafter "Chapter 2"]).
94. As Saul states: "[Direct democracy] is the ideal consummation of the rational as irrational, of the anti-democratic posing as democracy. The complex issues of reality, which democracy can deal with in its own slow, indirect way, are swept aside by single, clear issues" (*supra* note 86 at 109).

Human Rights Research and Education Centre, demonstrate the seductiveness of this reasoning:

> It is suggested that the need to promote consensual alliances with stakeholders will be critical in dealing with... even privacy concerns on the Internet.... It will require, in effect, a new form of governance of society where what are to be the fundamental shared values that a democratic society has not only the right, but also more importantly *the ability* to enforce, are ordained not by the elite, *but agreed upon by consensual alliances of citizens' groups, the private sector, and traditional governmental mechanisms.*[95]

The Act was created by group negotiations and multistakeholder consensual alliances, as the then Industry Minister John Manley[96] and Industry Canada's official documents[97] proudly assert.

The Act demonstrates that the process of direct consultation, negotiation and consensus-building legitimize the decisions of informal private governments without actually addressing concerns that conflict with the elite consensus. Citizens' voices may have been heard, but they were systematically ignored in the final formulation of the Act. The divergence

---

95. E. Mendes, "Democracy, Human Rights and the New Information Technologies in the 21st Century – the Law and Justice of Proportionality and Consensual Alliances" (1999) 10 N.J.C.L. 351 at 367.

The promotion of initiatives like 'Team Canada' (where corporations and government travel together abroad to create international networks) is used as an example of the democratic and egalitarian efforts of the federal government. It states:

> Another feature of the changing scene in Canada is the *democratization* of foreign policy... Foreign affairs are less and less an exclusive concern of the federal government and more and more a "Team Canada" effort. [emphasis added]

Canada, Special Joint Committee of the Senate and House of Common Reviewing Canadian Foreign Policy 1994, *Canada's Foreign Policy: Principles and Priorities for the Future* (Ottawa: Publications Service, Parliamentary Publications Directorate) [emphasis added].

96. "We started public consultations on the need for privacy legislation in 1994. We announced our intent to legislate in 1996 and we sought public comment on proposals for the legislation in 1998. These consultations overwhelmingly supported the use of the CSA standard as a basis for private sector privacy legislation." (Issue 5 Senate hearings, *supra* note 37)

97. In justifying the use of the CSA Standard in the Act the document states: "The Standard demonstrates the continued commitment of participating parties to fair information practices .... The result of cooperation among a wide cross-section of interest groups, it is truly a remarkable achievement." (ECOM4, *supra* note 8) And further commentary:

> The protection of personal information is achieved by bringing into law the Canadian Standards Association Model Code for the Protection of Personal Information. The CSA Standard was developed in a consensus process that included representatives from a broad spectrum of interests including industry, the public sector, consumer groups and labour organizations.

Senate, Standing Committee on Social Affairs, Science and Technology, Evidence, issue 1 (25 Nov. 1999) at 13.

of citizens' expectations of the content of the Act (broadly based privacy protection) and its actual substantive provisions (focusing on data protection) demonstrate this. As the Standing Committee concluded:

> Everywhere the Committee traveled, participants in our townhall discussions asked that the government create a legal framework to establish ground rules for the protection of privacy . . . . We do not believe that Canadians want ground rules to protect *only* their informational privacy, leaving the rest of their privacy rights to languish in a lawless frontier.[98]

The divergence of citizen expectations and the reality of the statute ultimately enacted are convincingly portrayed by the results of the public consultation conducted in 1998 by Industry Canada[99] and the writings of legal academics.[100]

---

98. Standing Committee, *supra* note 3 at 25 [emphasis added].

99. Some may argue that consensualism and compromise mean that no party leaves negotiations satisfied, hence both business and citizens sacrificed some interests to ensure the Act was created. The consultation paper produced by Industry Canada indicates clearly that throughout the process of creating the Act citizens have not been satisfied by its results, whereas corporate interests have generally been fulfilled.

The consultation document categorizes the responses to the preliminary Act by responses received from Privacy Commissioners, Consumer Groups (including organized labour), Telecommunications and Cable Sector, the Financial Sector, Commercial and Retail Organizations, Information Technology Associations, Individuals (including consultants, experts and academics) and other groups.

The report stated that "Privacy commissioners, consumer groups and individuals favour *greater precision*... In contrast, the majority of business organizations would prefer to see the CSA Standard adopted *without any changes*. Their view is that... more onerous requirements could stifle private sector activity."

Specifically, the report concludes that "All privacy commissioners support statutory privacy legislation, but *all* view the CSA Standard as requiring substantive improvements if it is to become the basis for privacy law." Almost two pages of recommendations of changes follow.

As for consumer groups, the report states: "All consumer organizations support a federal private sector privacy law, but *none believe the CSA Standard is currently sufficient* as a basis for legislation." The submissions of individuals concurred: "No individual thought the CSA Standard was sufficient without changes." Most tellingly, the report then lists three pages of substantive changes recommended by individuals and consumer groups that would have fundamentally altered the form and nature of the legislation. The most significant recommendation of the consumer groups was that of adding a right of privacy to the *Canadian Charter of Rights and Freedoms*. Individual recommendations included: adding principles from the Privacy Charter, incorporating six principles from the Australian Privacy Charter, reflecting the fair information practices of the Quebec Act, clarifying consent, limiting information collection to the absolute minimum required, requiring that information can only be collected directly from the individual, including a right to self-determination of health records and prohibiting surveillance except for law enforcement purposes.

In contrast, the summarized submissions of the business community are contained in two pages with few suggestions of changes to the legislation (*supra* note 5).

100. See also U. Franklin, "Stormy Weather: Conflicting Forces in the Information Society", presentation September 19, 1995 at the 18th International Conference for Privacy and Data Protection, Ottawa, online: Office of the Privacy Commissioner <http://www.privcom.gc.ca/english/02_05_a_960918_05_e.htm> (date accessed: 13 May 2001) [hereinafter "Stormy Weather"].

2. *The Consumerization of Citizenship*

If government is managed by non-citizen groups, their entitlement to public goods and services must be justified in the marketplace rather than through the democratic rights and obligations that only citizens can possess. The market both equalizes the rights of business and individuals and reduces the individual to the role of a 'stakeholder' or 'consumer' who must consume goods, as opposed to debating, arguing and exercising rights. As Ursula Franklin states,

> [w]hile those who primarily locate themselves in the human rights climate speak about citizens ... those who use the market language speak primarily about stakeholders. And when one speaks about rights and obligations, the other speaks about binding contracts.[101]

Government may perceive its function, then, as fulfilling the market needs of its stakeholders instead of legitimizing the democratic rights of its citizenry. This governmental role robs from citizens the only mechanism (democracy) through which they can meaningfully exercise collective power.

The use of terms such as "customers", "consumers", "clients" and "stakeholders" to describe interactions of citizens with government services and institutions further affirms the consumerization of citizenship. The use of these terms is not merely ideologically offensive – it is inaccurate. Citizens can be neither the customers nor clients of public services since citizens are in fact their employers; this relationship "is not tied to purchase or value for money, but to responsibility."[102]

Consumerism renders citizens into tractable subjects, making them uninterested in challenging abrogations of their rights. In a society where personal information is collected for the purposes of niche marketing and analyzing consumer preference, the market is portrayed as a sort of "Santa Claus: be good and you'll get your presents."[103] Unlike historical surveillance states, this new power is not used in an overtly coercive manner, which "instinctively repels most people."[104]

---

101. *Ibid.* at 2.

102. *Supra* note 86 at 96. The most accurate term to describe a citizen in the corporatist model would be 'shareholder' however even this term is inaccurate since citizens realize no monetary profits from their investment of taxes nor can those shares be bought and sold.

103. R. Whitaker, "Commentary on Gregory J. Walters, 'Digitizing Technology, Transforming Ourselves'" (1999) 10 N.J.C.L. 437 at 440.

104. *Ibid.* at 440. Whitaker has pointed out that the surveillance society effects the same results as a surveillance state. Corporations in a surveillance societies are risk averse. The consequence of presenting a risk (determined through surveillance) is exclusion from the marketplace. As Whitaker states: "those excluded by the surveillance society find themselves pretty much in the same position as those excluded by the security screening of the surveillance state." (*Ibid.* at 441).

The discourse of "stakeholders" and "consumers" permeates the creation of the Act, involuntarily demonstrating the substitution of citizens with rights by consumers with needs. The legislation should be "consumer friendly",[105] and will require "consumer" (not *public*) education.[106] The CSA Standard represents a consensus among "stakeholders"[107] where the needs of business to collect and the "consumer's" need (not right) to be informed must be balanced.[108]

3. *The Effects of Consumerism on Governmental Decision-making*

Perceiving citizens as consumers in a marketplace allows legislators to ask narrow questions that lead to particular answers. As Ursula Franklin states,

> [t]hose who deal primarily in the language and the forces of the market, see the world as becoming more and more a transparent, interlinked production site. Those of us who primarily come from, and are nourished in the tradition of human rights and justice, have a view of the world that hopefully makes the world more and more like a garden in which we all can walk, and in which we all have to be vigilant about the weeds, the plants, and the behavior of all those who use the garden for food, living, habitat and recreation.[109]

Government decision making promotes the appearance of problem-solving and administrative efficiency over results by focusing on self-interest instead of the public good, and the market instead of the human rights of citizens. Being seen to solve a problem is more important than its genuine final resolution. The production site which legislation seeks to regulate is managed by the "rational" judgment of technocrats and experts who can best predict its growth.[110] The short-term solutions that result from self-interested decision making are ultimately destructive of society since they are not broadly based on a shared vision of society.[111]

---

105. Supra note 89.
106. *Ibid.*
107. *Ibid.*
108. Industry Canada, "Privacy: The protection of personal information", online: Strategis <http://ecom.ic.gc.ca/english/privacy/632d6.html> (publication date: 8 November 2001).
109. Stormy Weather, *supra* note 100 at 2.
110. *Supra* note 86 at 102.
111. *Ibid.* at 33.

The Act is the predictable product of a technical, method-oriented approach which is not responsive to the broader policy concerns that should engage government. As the Standing Committee confirms,

> [c]onsequently, the protective framework we are proposing here [the Privacy Charter] will capture the full breadth of privacy, like a wide angle lens taking in a panoramic view, as opposed to the data protection framework toward which the Industry and Justice Ministers are working that focuses, *like a close-up lens, tightly on informational privacy rights.*[112]

In its pursuit of process and method, the government has neglected what it claimed to be the broader policy purpose of the Act (to protect privacy). It has created a "light, regulatory framework which does not impose a heavy burden on industry."[113] Citizens must vigilantly protect themselves against the rights that have been granted to non-citizen business and guard against the conformist influence of their status as 'consumer'.

4. *The Protection of Human Rights: Lost in the Commodity Shuffle*

The protection of personal information as a market commodity results from the consumerization of citizenship, reliance on the market to mediate disputes and the focus on method and self-interest. Short-term results ensue, minimizing or negating the human right to privacy. The commodification of information objectifies human interactions, fragments communities and molds social relations to the market model by relegating information, whose free exchange is vital to the creation and maintenance of communities and relationships, to the status of a market good.[114]

---

112. Standing Committee, *supra* note 3 at 25. [emphasis added]

113. As Industry Canada states: "In a light regulatory framework which does not impose a heavy burden on industry, consumer education is especially important to ensure that citizens are well informed about their privacy rights and are vigilant in protecting them" (*supra* note 89).

114. The flow of information in a community has been analyzed to consist of gift, threat and exchange information. All three types of information flow must occur in a healthy society, however the market model enables only the exchange of information. Kenneth Boulding has warned that, as a result, we face economic and social break-down since the commodification, not integration, of social relationships reduces our sense of community:

> The instability of capitalism may arise partly out of certain technical defects of an elaborate exchange system that results in unemployment and depression; it also results, however, from certain delegitimations of exchange, which may well arise because of strong preferences for integrative relationships, which are, after all, personally much more satisfying than exchange. To do things for love always seems to be more moral and progressive than to do things for money ... capitalism undermines itself... because of the failure of exchange institutions, such as finance, banking, corporations, and so on, to develop an integrative matrix that will legitimate them.

K. Boulding, *The Economy of Love and Fear: A Preface to the Grants Economy* (Belmont, California: Wadsworth Publishing Company, 1973) at 110.

A focus on data protection that constructs personal information as a commodity misrepresents the nature of information. Information enjoys unquestioned commodity status in the 'high-tech' economy. Upon closer inspection it may not be so easily classifiable. Robert Babe, a prominent Canadian communications scholar has argued that information is immaterial – what is quantifiable is the medium through which it is transmitted (*i.e.* bits of data, pages of text). Hence "[t]he disembodied or incorporeal character of information presents difficulties for economic analysis."[115] Information's value and the interpretation of its content vary according to the characteristics of source and receiver; thus, information depends on relationships and interactions and is difficult to define objectively.[116] Information is infinitely reproducible, indivisible and can be used without reducing its availability. It is also difficult to commodify information as it cannot be valued without information, which then itself cannot be valued without information leading to an infinite regression.[117] Arguably, while information possesses characteristics which allow it to fit within the box of "market goods", it should also be firmly planted in the garden of 'human rights'.[118]

---

115. Babe, *supra* note 93 at 16.

116. Even Industry Canada recognizes this when it states:

> Ideas and information exhibit very different characteristics from the goods and services of the industrial economy . . . the social value of ideas and information increases to the degree they can be shared with and used by others . . . . The more such items [ideas, information, innovation] are produced, the greater the social return on investment.

Industry Canada, Chapter 6: An Information Highway for Jobs and Growth, Strategis online: <http://strategis.ic.gc.ca/SSG/ih01644e.html> (publication date: 8 October 2001).

117. See generally Babe, *supra* note 93 at 11, 205.

118. Strong forces counter the consideration of information as a human right. For example, if information is considered a human right, then Southern 'developing' nations could insist on a "free and balanced flow" of information. These nations would not then have to export large quantities of food and resources to pay for Western information (enclosed through intellectual property law) that is crucial for development. Information as a human right would severely diminish profits of transnational corporations, hence is unlikely to gain wide currency. (*Ibid.* at 44.)

The following excerpt foreshadows the resistance of business to the specific proposal by Senator Finestone to "enshrine Canadians' right to freedom from surveillance [and] *the use of personal data* by others":

> An expert in Internet law warned the proposal would be seen as a handicap by Canadian businesses trying to use the Internet. "*Business would see it as an impingement on their rights*," said Michael Geist, a law professor at the University of Ottawa who specializes in the Internet.

Online: The Canadian Parliament <http://www.parl.gc.ca/cgi-bin/36/pb_gob.pl?e> (date accessed: 5 November 2000).

Shifting the debate about the privacy of personal information away from the commodification of information[119] has been broadly supported by the Standing Committee[120] and in particular by Paul-André Comeau, Privacy Commissioner of Quebec, who warned at the committee hearings,

> [i]t is dangerous and, at any rate, it could be very harmful for Canadians to see a debate focusing solely on the commercial value of information pertaining to privacy. Of course this information does have a commercial value, but it is first and foremost a question of basic rights.[121]

If information is not unequivocally a commodity, then its receivers should not be so readily called consumers. If receivers are not best seen as consumers then they should once again be regarded as citizens who have rights. It is then that the discourse shifts to consider human rights,[122] in particular the right to privacy of personal information.

Privacy is a polymorphous concept that is notoriously difficult to categorize. Four major features have been identified.[123] Privacy exists as an expression of personality or personhood and of personal autonomy. It also encompasses the right to arrange one's relationships by controlling information about oneself. Finally, privacy may also consist of "secrecy, anonymity and solitude."[124]

In the Canadian context, the right of privacy is given more substance but no clear definition materializes. In the words of the Standing Committee "privacy is reflected through many lenses. What emerges is a consensus which consists of a rainbow of values, interests, knowledge and experiences."[125] Canadians perceive privacy as a fundamental societal right that is necessary for the exercise of other rights (such as freedom of expression).[126] Privacy is grounded in dignity and autonomy and is an integral part of our society's collective value system. Functionally, privacy leads to a more transparent, candid and open society by nurturing and enabling

---

119. The approach adopted by the drafters of the Act (*supra* note 113).
120. Standing Committee, *supra* note 3 at 5.
121. *Ibid.* at 6.
122. The Standing Committee adds:

> [I]f we approach privacy issues from a human rights perspective, the principles and solutions we arrive at will be rights-affirming, people-based, humanitarian ones. On the other hand, if we adopt a market-based or economic approach, the solutions will reflect a different philosophy, one that puts profit margins and efficiency before people, and may not first and foremost serve the common good.

Ibid.
123. F.H. Cate, *Privacy in the Information Age* (Washington: Brookings Institute, 1997) at 19.
124. *Ibid.*
125. Standing Committee, *supra* note 3 at 1.
126. *Ibid.*

relationships within communities.[127] Its protection by government expresses a vision or policy of society.[128]

The Standing Committee has attempted to give legislative substance to the right of privacy through the Privacy Charter.[129] The Act falls short of its ostensible goal to protect privacy (see 'Purpose', section 3) when measured against the standards of both the Canadian Privacy Charter and the Australian Privacy Charter.[130] Most importantly, the Act creates no binding obligations – instead its substantive privacy protections are only recommendations.[131] Thus the Act violates provision 1.2 of the proposed Privacy Charter which guarantees that "those privacy rights will be respected by others adopting whatever protective measures are most appropriate to do so."[132]

The Act weakly enforces s. 1.2 of the Privacy Charter which proposes that "violations of these privacy rights . . . will be subject to proper redress."[133] Under Principle 4.9 (in particular 4.9.5) of the Act, if individuals successfully challenge the accuracy of information about them then the organization 'shall' amend the information. However, if the individual is not satisfied with the proposed amendment, then the organization is merely recommended to *record* the substance of the dispute.[134] Principle 10 recommends that organizations establish procedures to 'receive and respond' to complaints about compliance with the Act. An individual can file a complaint with the Commissioner if an organization fails to follow a recommendation in Schedule I[135] but can only apply to the Federal Court for a hearing after receiving the Commissioner's report. The obligation to redress privacy violations is placed on the citizen. This situation seems inequitable when one considers that the government could have directly assumed the obligation for

---

127. Response, *supra* note 59 at 447.
128. *Ibid.* at 449.
129. Privacy Charter, *supra* note 59.
130. I have chosen to compare the Act to the Canadian and Australian Privacy Charters, as opposed to the EU directive, because I believe that both Charters more accurately reflect the Canadian perspective on privacy protection (this conclusion derives primarily from the Standing Committee's results) and are distinctly not the product of the consensual alliance process of decision-making that I critique. Also, other authors have exhausted the comparison of the Act to the EU Directive. I will refer to the provisions of the Australian Privacy Charter when they differ or provide a useful definition for provisions of the Canadian Privacy Charter. (Response, *supra* note 59)
131. *Supra* note 2, s. 5.
132. Response, *supra* note 59. The Australian Privacy Charter contains similar language to the Canadian Privacy Charter: "Australians value privacy, They expect that their rights to privacy be recognised and protected." (*Supra* note 61.)
133. A similar provision is contained in Principle 4 of the Australian Privacy Charter.
134. *Supra* note 2, Sch. I, principle 4.9.6.
135. *Ibid.*, s. 11.

enforcement through the commonly established licensing or registration regime, complemented by a mechanism to investigate and prosecute (similar to enforcement under the *Human Rights Act*).[136] No right of enforcement is directly provided against the organization which is under no binding duty to resolve the dispute or respond to the complainant in a timely manner. There is no right to directly appeal the organization's response. Access to court is restricted until after the lengthy process of investigation (up to one year) is completed by the Commissioner.

Section 3 of the proposed Privacy Charter outlines six primary "duties" to ensure that privacy rights have been "adequately respected." Recommendations fail to create the 'duties' required by s. 3.1 of the Privacy Charter. The Act does not even address two of the duties contained in s. 3 of the Privacy Charter. In particular, there is no duty to "use and provide access to privacy enhancing technologies"[137] nor is there any guarantee that privacy protection be built into technological design.

Section 3.1 mandates a duty to secure meaningful consent. The Australian Privacy Charter stipulates that "'consent' is meaningless if people are not given information or have no option but to consent" as well as requiring that individuals have a right to withdraw their consent.[138] On the positive side, Principle 4.3.2 of the Act specifically addresses how consent becomes meaningful when the individual can reasonably understand the purposes for which the information will be used.[139] Meaningful consent is also promoted by Principle 4.3.3 which provides that consent cannot be given beyond the purposes for which that information will be used. As well, consent shall not be obtained through deception[140] and individuals are allowed to withdraw consent.[141]

However, the existence of meaningful consent is diminished by Principles 4.3.0, 4.3.1 and 4.3.4-7. Consent does not have to be obtained

---

136. The government could have adopted a much more stringent enforcement procedure involving either registration or licensing, models adopted in European countries. The 'data commissioner' model is perceived to be an intermediate level of data protection. A registration scheme would require the public and private sector to register their databases with a federal government agency. Government agencies can then regulate and de-register databases as they see fit. A licensing scheme requires prior government approval of all database uses. (Managing Privacy, *supra* note 10 at 212.) See also Standing Committee, *supra* note 3 at 19.

137. There is a reference in Principle 4.7.3 to the use of technological measures to protect information. *Supra* note 2, Sch. I.

138. *Supra* note 61, Principle 2.

139. In Schedule I this is termed the "knowledge and consent" requirement (*Supra* note 2, Sch. I. principle 4.3.2).

140. *Ibid.* principle 4.3.5.

141. *Ibid.* principle 4.3.8.

where it would be inappropriate,[142] in particular where a third party has no direct relationship with the individual.[143] Consent is not sought in those situations because it would be 'impractical' for the third party. This exemption potentially engulfs the rule since as more personal information is collected, exchanged and combined a larger proportion of it falls into the hands of third parties for whom it is impractical to seek consent from the individual concerned. It is not specified who decides or on what basis consent is deemed to be inappropriate. The Schedule contains no provision similar to that of the Australian Privacy Charter which requires that "[c]ollection should be from the person concerned, if practicable."[144] In addition, consent can be obtained after information is collected.[145] Hence, individuals can have information collected for one purpose and can then be asked to consent to another use of the information when the information is no longer within their control.[146]

The form of consent required varies with the type and circumstances of the information[147] and, in particular, implied consent is said to be appropriate when information is "less sensitive".[148] Consent that is implied and not express is not meaningful in this context.[149] In addition, there is a wide and arbitrary discretion given to organizations to determine when a particular use of information is 'less sensitive'. Specifying that medical and income records are more sensitive than the names and addresses of subscribers to a magazine[150] fails to adequately substantiate this discretion. Additionally, what may be a less sensitive use of personal information to an organization may not be considered less sensitive to an

142. *Ibid.*, principle 4.3.0.
143. The Schedule uses the example of a "charity or direct marketing firm that wishes to acquire a mailing list from another organization" (Note - *ibid.* principle 4.3.0).
144. *Supra* note 61, principle 11.
145. *Supra* note 2, principle 4.3.1.
146. Note that Principle 4.2.4 recommends that consent be obtained if information is used for a new purpose. *Ibid.*
147. *Ibid.*, principle 4.3.4.
148. *Ibid.*, principle 4.3.6. Note as well that there is no statutory definition of informed consent even though one is provided in s. 2.1.0 of the CSA Code.
149. The Standing Committee has specifically addressed this issue, stating: "We do not believe that consent to privacy invasions should ever be implied." (Standing Committee, *supra* note 3 at 24) Principle 2 of the Australian Privacy Charter stipulates that meaningful consent requires full information. (*Supra* note 61.)
150. *Supra* note 2, pinciple 4.3.4.

individual.[151] Further, there is no obligation that consent be freely given and independent of coercion.

The Act also provides that consent can be given by negative implication, which like implied consent, is not meaningful since it has not been expressly given with full knowledge.[152] Individuals are not warned if they fail to give consent when consent is required. If consent is withdrawn then an organization is only advised to inform the individual "of the implications of such withdrawal" (*i.e.* that if consent is withdrawn then there is no consent).[153] However, there is no requirement that the organization respect the withdrawal of that consent or even act upon it.[154]

The standard of consent that I suggest is common in other spheres, for example, in the criminal law. Relevant consent provisions in s. 273.1 of the *Criminal Code* hold, for example, that,

> No consent is obtained, for the purposes of [sexual assault, aggravated sexual assault or sexual assault with a weapon] where . . .
>
> (c) the accused induces the complainant to engage in the activity by abusing a position of trust, power or authority;
>
> . . .
>
> (e) the complainant, having consented to engage in sexual activity, expresses by words or conduct, a lack of agreement to continue to engage in the activity.

The criminal standard of consent requires that the consent must be both voluntary, affirmatively given and activity specific. Consent cannot be implied as a defence to sexual assault. Consent can be withdrawn at any time and that lack of consent must be immediately respected.[155] *R.* v. *Ewanchuk* further holds that claiming silence, passivity or ambiguous conduct show consent to sexual acts is not a defence to sexual assault. Although the context of data protection is very different from that of

---

151. For example, a person's social insurance number indicates whether they are a recent immigrant. An individual may not wish to disclose this information when applying for a job to avoid discrimination.

152. *Supra* note 138. Principle 4.3.7 (b) provides that if one does not check a box that would prevent information from being given to another organization, then consent has been given. This type of consent led to a large outcry in Canada in January 1995 when the cable television industry introduced new cable television services to all its customer at an increased cost and consumers had to write to specifically request not to be provided those services. For more information see online: Industry Canada, <<http://strategis.ic.gc.ca/SSG/ca00887e.html>> (date accessed: 8 May 2001).

153. *Supra* note 2, Sch. I, principle 4.3.8.

154. For example, there is nothing to prevent an organization from stating that the implication of the withdrawal of consent is that nothing changes with respect to that information.

155. *R.* v. *Ewanchuk*, [1999] 1 S.C.R. 330.

sexual assault, the criminal definition of consent can be used as a framework for obtaining meaningful consent.

Section 3.1 of the Privacy Charter requires that if privacy rights must be infringed, then the means must be minimally impairing. Specific provisions of the Act can be identified that attempt to minimally impair the infringement of privacy rights. The collection,[156] use and disclosure of personal information is limited to identified purposes[157] and information can only be retained for "as long as necessary for the fulfilment of those purposes."[158] However, organizations are only required to document (not inform individuals) of the use of personal information for new purposes.[159] There is no provision in the Act, as in the Australian Privacy Charter, that a "*minimum* amount of personal information should be collected."[160] Additionally, the Schedule suggests that organizations establish maximum and minimum retention period for information, without providing a strict standard of what those retention periods should be.[161] Personal information that is no longer useful should be "destroyed, erased, or made anonymous."[162] This provision incorrectly equates making information anonymous with destruction. Merely removing an identifier from data allows it to be recycled in another form.

The duties to be accountable and transparent provided for in section 3.1 of the Privacy Charter[163] are implemented in the Act to a greater degree than are the other duties of the Privacy Charter. The Act provides that organizations must designate individuals to be accountable for their compliance with the principles of Schedule I.[164] The organization must develop procedures to protect personal information and to "receive and respond to complaints and inquiries."[165] However, accountability is merely a public relations façade if there is no enforceable standard of a right to privacy which can be used to challenge procedures and poor responses to complaints.

Transparency requires that the purposes of personal information use be identified,[166] documented[167] and specified to the individual from

---

156. *Supra* note 2, Sch. I. principle 4.4.1.
157. *Ibid.*, principle 4.5.0. The Australian Privacy Charter contains a similar provision in Principle 11.
158. *Ibid.*, principle 4.5.0. The Australian Privacy Charter has no provisions respecting the retention periods of personal information.
159. *Ibid.*, principle 4.5.1.
160. *Ibid.*, principle 11, Australian Privacy Charter [emphasis added].
161. *Ibid.*, principle 4.5.2.
162. *Ibid.*, principle 4.5.3.
163. *Ibid.*, principles 3 and 5 of the Australian Privacy Charter.
164. *Ibid.*, principle 4.1.0.
165. *Ibid.*, principle 4.1.4(a-b).

whom the information is collected.[168] Schedule I, however, does not create a positive duty which requires that the purpose will actually be communicated to the individual. This is evident from the fact that the Schedule does not require more than "specification" and that persons collecting information "should" be able to explain the purposes of collection.[169] As well, there is no requirement that the purpose for information collection be assessed to be valid or reasonable or that the purpose be justified.

Transparency is also addressed through the principle of openness about an organization's management of personal information.[170] However, the term management is ambiguous. Does it relate to use or merely collection of personal information? What degree of detail will be available? Transparency, once again, is not sufficient to protect privacy if there are no effective means to enforce privacy rights under the Act. As well, there is no requirement in the Act similar to Principle 13 of the Australian Privacy Charter which creates a positive duty for organizations to "make people aware of the existence of personal information held about them." A legislative focus on method at the expense of content is demonstrated by the focus of the Act on procedural rights like accountability and transparency and its legislative treatment of more substantive rights to privacy (*e.g.* consent).

The Act does not address the specific rights to ownership and anonymity of personal information provided for in section 4.1 of the Privacy Charter.[171] There is no protection in the Act of the autonomy interest protected by ownership of personal information.[172] The sensitivity (and presumably anonymity) of data varies with the source from which it is collected;[173] however, this sensitivity is only protected through safeguards designated at the discretion of the organization.[174] It is problematic that determining the level of protection is placed at the discretion of the

---

166. *Ibid.*, principle 4.2.0.
167. *Ibid.*, principle 4.2.1.
168. *Ibid.*, principle 4.2.3.
169. *Ibid.*, principle 4.2.5.
170. *Ibid.*, principle 4.8.
171. The Australian Privacy Charter does not provide for a right to ownership of personal information. However, the Charter protects anonymity in Principle 10, which stipulates that "people should have the option of not identifying themselves when entering transactions." (*Supra* note 61.)
172. I propose that ownership be interpreted (in the spirit of the Standing Committee's report) as those who possess the right to enforce the obligations outlined under the Privacy Charter as opposed to an affirmation of the commodity status of personal information.
173. *Supra* note 2, Sch. I, principles 4.3.4, 4.7.2.

organization who will pay the increased costs of that security. There is no specific recommendation in the Act that personal information be treated as confidential or anonymous and organizations are merely recommended to inform their employees of the confidentiality of personal information. There is no requirement that a confidentiality agreement be completed if information is transmitted to a third party.

The obligations under section 5 of the Privacy Charter, as the Standing Committee reports, are primarily those recognized under the CSA Code.[175] However, the Act does not address two of the obligations under s. 5 (that are also not contained in the CSA Code). First is the duty to hold sensitive information in trust. This obligation protects anonymity and relationships by mandating that collectors of medical, financial or genetic information should be held to the higher standard of care of "trusteeship" with respect to the handling of that information.[176] Secondly, the Act does not protect individuals from adverse effects if they choose to exercise their privacy rights. Such a provision would protect the autonomy of individuals by forbidding the provision of inferior service, no service or increased costs for a service if individuals refuse to provide personal information.[177]

By comparing the Act to the provisions of the Privacy Charter and the Australian Privacy Charter, it becomes evident that the government has failed to emerge from its narrow analysis of data protection to meaningfully fulfill the obligations of a right to privacy. The substantive privacy protections of the Act are recommendations not obligations; citizens are not provided with adequate means of redressing violations; there is no duty not to disadvantage people when they choose to exercise their rights to privacy; consent is not required to be meaningful; there is no declaration that individuals are the owners of their personal information nor is there any general provision that personal information is confidential. As a result, the Act may address the needs of consumers whose interests must

---

174. *Ibid.* principle 4.7.

175. Standing Committee, *supra* note 3 at 25.

176. The Supreme Court of Canada explicitly found a duty to hold sensitive medical information in trust in *McInerney* v. *MacDonald*, [1992] 2 S.C.R. 138.

177. Standing Committee, *supra* note 3 at 25. Although Principle 4.3.3 attempts to address this concern, it only recommends that organizations shall not require consent to the "collection, use, or disclosure of information beyond that required to fulfil the *explicitly specified, and legitimate purposes*." Thus organizations can refuse access to products or services if a person refuses to consent to the use of her information for the specified purpose.
The Australian Privacy Charter states in Principle 2 that "'consent' is meaningless if people . . . have no option but to consent in order to obtain a benefit or service." Also, the Charter stipulates that "a desire for privacy does not mean that a person has 'something to hide'. People who wish to protect their privacy *should not be required to justify their desire to do so.*" [emphasis added] (*Supra* note 61.)

be balanced with those of business, but it fails to protect citizens as individuals with rights to privacy.

5. *The Process of Legitimizing the Legislation: Sugar-Coating Bad Medicine*

The apparent acceptance of (or lack of audible protest to) the Act's data protection provisions results from a perception of technological development as inherent or inevitable. Technological determinism posits that technology evolves autonomously according to its own internal logic; societies must then adapt to the development of technology at all its stages (technological inevitability).[178]

The language of determinism pervades Industry Canada's documents which portray the "knowledge society" as the result of an unavoidable historical trend: "[during the industrial revolution] an urban manufacturing economy displaced an essentially rural and agricultural society. Now we are experiencing an equally profound shift to a knowledge-based economy."[179]

The "information society" is portrayed as not only historically necessary; it is also said to develop according to the unavoidable processes of evolutionary biology. In the words of the Information Highway Advisory Council (IHAC) "the information economy is still in its *infancy.*"[180] However, "[t]he technology and information infrastructure will be the *central nervous system* of the new economy and society"[181] where "the knowledge, information, data and services traveling the Information Highway" will form "the *lifeblood* of the knowledge based economy."[182]

Technology that evolves like humans is also endowed with human abilities, such as the ability to engage in non-discriminatory expression:

---

178. A. Feenberg, *Critical Theory of Technology* (Oxford: Oxford University Press, 1991) at 123.

179. Chapter 6, *supra* note 116.

180. *Supra* note 89 [emphasis added].

181. Industry Canada, Chapter 1: Toward a Society Built on Knowledge, online: Strategis <http://strategis.ic.gc.ca./SSG/ih01639e.html> (publication date: 8 October 1997). [hereinafter "Chapter 1"] [emphasis added].

182. Chapter 6, *supra* note 116 [emphasis added].

"the Internet's most powerful feature is that it allows computers and networks to communicate openly and effectively, regardless of make . . . ."[183] However, in order to properly mythologize technology it must have superhuman powers: "Over the past three years, the Internet has begun to pervade the lives of many Canadians . . . . Ultimately *the technology promises to extend and improve dramatically* learning, health and other public services."[184]

Since technology is constantly evolving, Canadians have "no option but to vigorously embrace the development and dissemination of the new technologies." [185] The technological imperative[186] requires an urgent response as otherwise Canadians will find themselves falling further behind in the international race to improve productivity of all sectors of the Canadian economy.[187] We must be advised that "[a] social, economic and cultural revolution is now transforming the world" and "[a] new game is starting, and the older rules no longer apply."[188] Thus, "[r]apid technological advances *demand* that we formulate a legislative framework"[189] that outlines the new rules for the new game. Educational institutions must create workers for the technological society: "Computer and Internet literacy is a necessary precondition for success in the emerging knowledge society and economy . . . . All levels of government in Canada have been moving actively to ensure our educational institutions can fulfill this role."[190]

Not only must the economy adapt to the technological imperative, so too must human social interactions: "[p]hysical distance will disappear as

---

183. Industry Canada, Chapter 3: The Internet: Advancing the Information Highway, online: Strategis <http://strategis.ic.gc.ca./SSG/ih01641e.html> (date accessed: 8 October 1997) [hereinafter "Chapter 3"]. As well, [the Internet] has the potential to bring far-reaching benefits and changes to Canada's economic life and industrial structure. It can generate profound shifts in employment. It can create both global opportunities and a more competitive environment for Canadian companies....

184. *Ibid.* [emphasis added]. See *infra* note 195.

185. Canada, Hon. Francis Fox, Minister of Communications, *Culture and Communications: Key Elements of Canada's Information and Communications Infrastructure* (Ottawa: Supply and Services, 1983) at 5.

186. "We have been delighted by the energetic responsé of industry, individuals and community groups across the country to the *imperative of developing Canada's Information Highway*" (Chapter 1, *supra* note 181) [emphasis added].

187. *Ibid.*

188. *Ibid.*

189. *Supra* note 89.

190. Industry Canada, Chapter 4: Access: The Cornerstone of the Information Society, online: Strategis <http://strategis.ic.gc.ca./SSG/ih01642e.html> (publication date: 8 October 1997) [hereinafter "Chapter 4"].

a factor in human relations .... The creation, manipulation and sharing of information and knowledge will become an overriding human imperative."[191] Culture, too, must adapt to the inevitable technological transformation: "[a]rtists and creators need opportunities to develop their skills by using the most sophisticated technology."[192]

Technology does not self-propagate – it is funded, researched, controlled and disseminated largely by businesses.[193] Technology is owned and developed, and its use generates a divisible profit.[194] If technology is perceived to be inevitable then citizens must adapt to the changes instead of attempting to control those changes and question the distribution of benefits from those changes. Thus the Act is necessary to outline the rules of the inevitable technological development that is required to secure economic and social security in Canada. Canadians must, in their best interests, surrender their personal information as fuel for the 'knowledge economy' without directly receiving any of the profits business acquires from its use. Government and industry have failed to ask many vital questions. Does technology lead to economic and social security? This question is critical in light of economic measurements that are unable to demonstrate an increase in productivity or market efficiency due to the increased use of technology.[195] Do Canadians want a society which gives technology such prominence?[196] Are new technologies appropriate or necessary or even reasonably justifiable in a free and democratic society? Do Canadians really want new technologies or their products, such as

---

191. *Supra* note 181.

192. Industry Canada, Chapter 5: Canadian Content: Creating an Information Highway for Canadians, online: Strategis <http://strategis.ic.gc.ca./SSG/ih01643e.html> (publication date: 8 October 1997) [hereinafter "Chapter 5"].

193. For an interesting study of how the development of the information highway is firmly controlled by Canadian corporations see Babe, *supra* note 93 at 199.

194. *Supra* note 88.

195. Legislators ignore the well-documented productivity paradox – that, for example, service industries spent $860 billion in the 1980's on technological solutions to improve their productivity. However, their productivity only increased by 0.8% per year (E.con, *supra* note 62 at 244). IHAC attempts to dismiss the productivity paradox by blaming the measurement tools: "the federal government should continue its national and international efforts to *create useful economic and social indicators*. This work should proceed as rapidly as possible".[emphasis added].(Chapter 6, *supra* note 116.) Thus, technology provides economic benefits – we just cannot measure them.

196. As the Standing Committee reports: "participants felt that we will be unable to find the appropriate balance [between civil society and technology] if we 'continue to allow technology to be the tail that wags the dog'" (*supra* note 3 at 4).

direct marketing?[197] Should the Canadian government be investing in technological or community-based solutions?

The passive response to the Act may result from the effects of the "Santa Claus market"[198] and the powerlessness engendered both by the governance of self-interested groups and the apparent inevitability of technological development. As well, citizens are poorly informed of the prevalence of technology (for example, surveillance technologies such as video cameras and ticket readers) and its capabilities. This lack of information is justified by the fact that informing the citizenry changes nothing if technological development is inevitable.[199]

However, the technological society prefers that citizens remain ignorant of the uses of their personal information[200] as most would demand greater protection for their privacy rights,[201] which would increase business costs. For example, the Canadian Privacy survey completed by Ekos concluded that respondents "would be more at ease with others using their personal information if they had control over this information, knew their privacy rights were protected and knew government exercised some form of oversight or monitoring of these activities."[202]

The names that government and industry have chosen to define the debate about privacy have silenced the voices of those who oppose its content. As Patricia Monture has stated, "[n]ot being in control of the process of naming – that is defining who you are – serves as one of the

197. A survey by Bell Canada found that 98% of customers found telemarketing to be "very annoying." As a response, the Canadian Direct Marketing Association provided a phone number that one could call to be removed from telemarketing lists. The service was so overwhelmed by calls it was shut-down (Free Enterprise, *supra* note 17 at 9).

198. *Supra* note 101.

199. Standing Committee, *supra* note 3 at 5.

200. Commenting on the results of citizen focus groups, in a study of 3 major Banks, a Life Insurance company, 2 major Health Insurance companies and a credit card company which examined those organization's privacy practices, the author commented:

> Thus, the focus groups often turned into an educational experience for the consumers . . . .
>
> As they learned more about the various policies and practices [of the corporations], many consumers because angry . . . .
>
> These findings stand as a stark reminder to industries handling sensitive personal information: if policies and practices are deemed offensive by consumers, simply providing consumer education about existing policies and practices may be a *counterproductive endeavour* [for business] [emphasis added].

Managing Privacy, *supra* note 10 at 149

201. This is recognized by Industry Canada when it proposes that consumers be educated so as to vigilantly protect their rights (*supra* note 113).

202. *Supra* note 37.

most express examples of silencing that I can think of."[203] The legislative acts of government have named the Act as the "privacy bill" not the e-commerce bill.[204] The management of personal information is called "data protection" and citizens have been named as "consumers". Rights are named as "market needs and desires" and private sector industry is referred to as a "stakeholder".

Thus the perception of technological inevitability discourages questions about the appropriateness of new technologies and justifies the ignorance of citizens about its uses. The government's power to name the terms of discussion effectively silences dissenting voices.

V. *Recommendations and Conclusions*

There is a sense of urgency surrounding the effective implementation of privacy rights in Canada.[205] I do not believe it is reasonable to recommend that the Act be repealed. However, there are three primary means through which privacy rights can be enforced. First, a right of privacy can be included in the *Canadian Charter of Rights and Freedoms.* Second, the Privacy Charter can be enacted as law and finally the Act can be amended to better protect Canadians.

1. *The Charter of Rights and Freedoms*

Privacy advocates have proposed including a right to privacy in the *Charter.*[206] Some advantages are that privacy would become a right that is enforceable by the courts. Its inclusion in the Constitution would grant it symbolic significance in Canadian law. However, there are disadvantages to the *Charter* approach. Privacy could only be included in the *Charter* by amending the Constitution, which is a notoriously difficult

203. "Reflecting on Flint Woman" in R. Devlin, ed., *Canadian Perspectives on Legal Theory* (Toronto: Emond Montgomery, 1991) 351 at 354.

204. A similar situation occurred when wiretapping provisions were introduced into the *Criminal Code* by the *Protection of Privacy Act*, S.C. 1973-74, c. 50 in 1974. After judicial comments, this section was renamed and included in the *Criminal Code* in Part VI under the title "Invasion of Privacy."

205. Highlighted by the Standing Committee (*supra* note 3) which states:

> As much as we found a sense of cautious optimism that it was not too late to protect our privacy, we encountered a clear sense of urgency. People across the country called on the government to act now or to risk losing the trust citizens have traditionally placed in our legislators to balance our social good with economic and political goals

On a different note, Industry Canada states: "The global challenge to compete in the electronic marketplace means we *do not have time* for a slow evolutionary approach to building up the protection of personal information and consumer trust." (*supra* note 8).

206. Such advocates include Bruce Phillips (former federal Privacy Commissioner), Members of Parliament David Crombie and Svend Robinson, the federal government itself in its 1979 proposal for the Constitution and Ann Cavoukian. (Ontario Information and Privacy Commissioner), online: Information and Privacy Commissioner/Ontario <http://www.ipc.on.ca/english/pubpres/reports/fine-01.htm> (date accessed: 8 May 2001).

procedure. Additionally, the Supreme Court of Canada, as outlined above, has defined ss. 7, 8 and 2(b) to include rights to privacy, dignity and autonomy. It is unclear what further protection would be effected by specifically including a right to privacy. A *Charter* right to privacy would only directly apply to government action and would be subject to a s. 1 justification. The time and expense of mounting a constitutional challenge make this option unattractive for regular and efficient enforcement.

2. *The Privacy Charter*

A second option is to enact a Privacy Charter as a Privacy Bill of Rights (both federally and provincially). This option is attractive, as it would constitute a broad policy statement by government that privacy deserves protection. The detailed codification of a right to privacy is an ideal means to greatly enhance the enforcement of that right.

Ideally, the Privacy Charter would be enacted as a Bill of Rights with quasi-constitutional status which would then be complemented by expanded funding and resources for the Privacy Commissioner. Individuals would bring complaints to the Privacy Commissioner who would investigate and prosecute violations of the Act (much like the Human Rights Commission).[207] In this ideal world, the Act would be repealed and replaced by a licensing scheme that would enable direct government supervision of information gathering activities.

3. *Improving the Act*

The most realistic means by which the protection of privacy may be improved would be to amend the Act, in light of the provisions of the proposed Canadian Privacy Charter (the ideal situation), the Australian Privacy Charter and the provisions of the Quebec Act.[208] The provisions of the Quebec Act are particularly influential as they are currently law and are widely considered to effect substantive protection of privacy rights in that province.[209]

The first major recommendation is to make the Schedule I provisions binding obligations instead of recommendations. To ensure this happens, a justification provision could be added which provides that infringements on privacy will be permitted only if they can be demonstrably justified in a free and democratic society. A general recommendation is that all

---

207. However, the creation of a separate scheme of human rights protection for privacy could be perceived as privileging privacy rights over rights contained within human rights codes and an unnecessary duplication.

208. *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1.

209. R. Côté & R. Laperrière, *Vie Privée Sous Surveillance* (Québec: Yvon Blais, 1994).

provisions should be made more specific. In particular, some of the most important prospective amendments to the Act and Schedule follow.

The current preamble to the Act should be amended to include a statement that the Act recognizes the right of privacy of individual with respect to their personal information to promote respect for the physical and psychological autonomy, integrity and dignity of individuals.[210] The Act should also clearly state in its preamble that the protection of privacy is currently threatened.

The Act, within its preamble or preliminary to further substantive provisions, should state that the provisions of the Act must be interpreted in light of:[211]

- A right to physical privacy
- A right to privacy of personal information
- A right to a personal space in which to conduct affairs,[212] not only in the home, but also "in the workplace, the use of recreational facilities and public places"[213]
- A right to be free from surveillance, where surveillance would be defined as including the monitoring of communications, movement and personal information except if required under the Criminal Code
- A right not to be disadvantaged because one chooses to exercise privacy rights. The exercise of those rights does not have to be justified.[214]

---

210. See *Morgentaler* and *Jones*, *supra* note 44.
211. Canadian Privacy Charter, *supra* note 59, s. 1.1.
212. The "zone of privacy" discussed in *Jones*, *supra* note 44.
213. Australian Privacy Charter, *supra* note 61, principle 8.
214. The Quebec Act contains such a provision:

> Section 9. No person may refuse to respond to a request for goods or services or to a request relating to employment by reason of the applicant's refusal to disclose personal information except where
>
> (1)collection of that information is necessary for the conclusion or performance of a contract;
>
> (2)collection of that information is authorized by law; or
>
> (3)there are reasonable grounds to believe that the request is not lawful.

An equivalent provision exists in the residential tenancies regime in Nova Scotia, where s. 20 permits the Director to "refuse to exercise, in favour of a landlord, the powers or authorities under this Act... [if it] is of the opinion that a landlord has acted in retaliation for a tenant attempting to secure or enforce the tenant's rights under this Act...." (*Residential Tenancies Act*, R.S.N.S. 1989, c. 401).

Accountability

The accountability provisions should require that files containing personal information about an individual must specify the categories of employees who will use and view the data[215] and the specific source of any information collected from a third party.[216]

Identifying Purposes

This section should include a declaration that personal information is owned by the subject, whose meaningful consent would be required for its use for specific purposes.[217] The provision should mandate a positive duty that the purpose of information use be communicated to the individual. The Act should expressly stipulate that individuals must be informed of uses of their information for new purposes. All purposes must be reasonably justifiable.

Consent

The consent provisions of Schedule I should be amended to include a provision similar to the Privacy Charter and s. 14 of the Quebec Act to provide that consent to the communication or use of personal information must be meaningful, free, and knowledgeable and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested. As well, the Act should stipulate that consent that is not meaningful, free or knowledgeable is not valid consent. [218] The Act should specifically prohibit implied consent, and particularly consent by negative implication.

A further provision should be added to vitiate consent when a technology does not serve the public good. A sample provision is contained in principle 2 of the Australian Privacy Charter which states that "[i]n exceptional situations the use or establishment of a technology or personal data system may be against the public interest even if it is with the consent of the individuals concerned."

The type of consent should not vary based on the sensitivity of information involved. However, if this provision remains in the Schedule, a precise definition of 'sensitive information' must be included. The Act should specifically stipulate that if consent is withdrawn then information must be erased or destroyed.

---

215. Section 8(2) of the Quebec Act requires that a person be informed of "the use which will be made of the information and the categories of persons who will have access to it within the enterprise." (*supra* note 52.)
216. *Ibid.*, s. 7.
217. Canadian Privacy Charter, *supra* note 59, s. 4.1
218. Quebec Act, *supra* note 52, s. 14.

Limiting Collection

Collection must be limited to an absolute minimum. Personal information should only be collected directly from the person involved.[219]

Limiting Use, Disclosure and Retention

Specific retention periods should be included. Principle 4.5.3. should be amended so that personal information that is no longer required should be "destroyed or erased" only and not made anonymous.

Accuracy

Personal information should not be as accurate as the purposes require; rather information should be as accurate as possible to ensure people are not disadvantaged by erroneous and outdated information.

Safeguards

A requirement should be added to the Schedule and the preamble of the Act that sensitive information be held in trust.[220] Additionally, the Act should specifically state that information will be held confidentially and that safeguards must be implemented to maintain confidentiality. Individuals should be entitled to demand that transactions occur and that information be held anonymously.[221]

Openness

The policy of openness should require organizations to inform people of the existence of information held about them.[222] The organization should be required, not only to make available specific information about the management of personal information, but information about specific uses, categories of employees who have viewed the information and the precise content of that information. This part should also include a general statement of policy that openness is needed to facilitate public participation in the protection of personal information.

Individual Access

This part should include a right to have information deleted and withdrawn.[223] Additionally, it should require that no fees should be charged to provide access to or amend data.

---

219. *Ibid.*, s. 6.
220. Canadian Privacy Charter, *supra* note 59, s. 5.1.
221. Australian Privacy Charter, *supra* note 61, principle 10.
222. *Ibid.*, principle 13.
223. See generally Quebec Act, *supra* note 52, s. 26.

Challenging Compliance

Individuals should be allowed to directly appeal or enforce the decision of an organization if he or she challenges the organization's compliance. The organization should be required to respond within a specific period of time (*e.g.* 30 days).[224] The cost of a challenge (including investigation and adjudication) should be borne either by the organization or the Office of the Privacy Commissioner, and advocacy services should be provided to individuals free of charge. Investigation should be conducted by the Office of the Privacy Commissioner.

The Act represented an opportunity for the government to affirmatively address Canadian citizens' concerns about the protection of their privacy. However, by viewing privacy protection principally through the lenses of the market and data, the Act ultimately better serves the interests of the market than those of human rights. Invasions of privacy by new and established technologies are neither necessary nor inevitable. Broad, democratic policy-making can ensure that citizens construct and guide the society in which they live by controlling the technologies that are used and developed. In order to do so, however, citizens must voice their concerns and governments must listen and effectively respond to ensure that the human rights aspects of privacy protection are substantively addressed, either through amendments to the Act or through the enactment of a Charter of Privacy Rights.

Appendix A

The Privacy Charter is as follows:

1.1 Everyone is entitled to expect and enjoy:

- Physical, bodily and psychological integrity and privacy;
- Privacy of personal information;
- Freedom from surveillance;
- Privacy of personal communications; and
- Privacy of personal space;

1.2 Everyone is guaranteed that:

- These privacy rights will be respected by others adopting whatever protective measures are most appropriate to do so; and
- Violations of these privacy rights, unless justifiable according to the exceptions principle which follows, will be subject to proper redress;

224. *Ibid.*, s. 32.

2. *Justification for Exceptions*
Exceptions, allowing the rights and guarantees set out above to be infringed, will only be allowed if the interference with these rights and guarantees are reasonable and can be demonstrably justified in a free and democratic society

3.1 The basic duties owed to others to ensure their privacy rights are adequately respected include:
- The duty to secure meaningful consent;
- The duty to take all steps necessary to adequately respect others' privacy rights or, if their rights must be infringed, to interfere with privacy as little as possible;
- The duty to be accountable;
- The duty to be transparent;
- The duty to use and provide access to privacy enhancing technologies; and
- The duty to build privacy protection features into technological designs.

4.1 Specific rights related to personal information
- Everyone is the rightful owner of their personal information, no matter where it is held, and this right is inalienable.
- Everyone is entitled to respect and enjoy anonymity, unless the need to identify individuals is reasonably justified.

5.1 The basic duties owed to others to ensure their informational privacy rights are adequately respected include, in addition to the general obligations set out above:
- The duty to hold sensitive personal information in trust;
- The duty to limit information collection to what is necessary and justifiable under the circumstances;
- The duty to identify the purpose for which personal informa tion is collected;
- The duty to ensure the information collected is correct and of the highest quality;
- The duty to provide the people whose personal data is collected with access to that information and a means to review and, if necessary, to correct it;
- The duty to only use and disclose personal information for the purposes identified when meaningful consent was obtained;
- The duty to keep personal information only for as long as is necessary and justifiable;
- The duty not to disadvantage people because they elect to exercise their rights to privacy.

Appendix B
AUSTRALIAN PRIVACY CHARTER[225]

Preamble

THE MEANING OF 'PRIVACY'

Australians value privacy. They expect that their rights to privacy be recognised and protected.

People have a right to the privacy of their own body, private space, privacy of communications, information privacy (rights concerning information about a person), and freedom from surveillance.

'Privacy' is widely used to refer to a group of related rights which are accepted nationally and internationally. This Charter calls these rights 'privacy principles'.

Privacy Principles comprise both the rights that each person is entitled to expect and protect, and the obligations of organisations and others to respect those rights.

Personal information is information about an identified person, no matter how it is stored (eg sound, image, data, fingerprints).

PRIVACY IS IMPORTANT

A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organisations to intrude on that autonomy.

Privacy is a value which underpins human dignity and other key values such as freedom of association and freedom of speech.

Even those privacy protections and limitations on surveillance that do exist are being progressively undermined by technological and administrative changes. New forms of protection are therefore required.

INTERFERENCES WITH PRIVACY MUST BE JUSTIFIED

Privacy is a basic human right and the reasonable expectation of every person. It should not be assumed that a desire for privacy means that a person has 'something to hide'. People who wish to protect their privacy should not be required to justify their desire to do so.

The maintenance of other social interests (public and private) justifies some interferences with privacy and exceptions to these Principles. The onus is on those who wish to interfere with privacy to justify doing so. The Charter does not attempt to specify where this may occur.

---

225. © Australian Privacy Charter Council, 1994, online: <http://www.anu.edu.au/people/Roger.Clarke/DV/PrivacyCharter.html> (date accessed: 23 March 2000).

AIM OF THE PRINCIPLES

The following Privacy Principles are a general statement of the privacy protection that Australians should expect to see observed by both the public and private sectors. They are intended to act as a benchmark against which the practices of business and government, and the adequacy of legislation and codes, may be measured. They inform Australians of the privacy rights that they are entitled to expect, and should observe.

The Privacy Charter does not attempt to specify the appropriate means of ensuring implementation and observance of the Privacy Principles. It does require that their observance be supported by appropriate means, and that appropriate redress be provided for breaches.

Privacy Principles

1 . JUSTIFICATION & EXCEPTIONS

Technologies, administrative systems, commercial services or individual activities with potential to interfere with privacy should not be used or introduced unless the public interest in so doing outweighs any consequent dangers to privacy.

Exceptions to the Principles should be clearly stated, made in accordance with law, proportional to the necessities giving rise to the exception, and compatible with the requirements of a democratic society.

2. CONSENT

Individual consent justifies exceptions to some Privacy Principles. However, 'consent' is meaningless if people are not given full information or have no option but to consent in order to obtain a benefit or service. People have the right to withdraw their consent.

In exceptional situations the use or establishment of a technology or personal data system may be against the public interest even if it is with the consent of the individuals concerned.

3. ACCOUNTABILITY

An organisation is accountable for its compliance with these Principles. An identifiable person should be responsible for ensuring that the organisation complies with each Principle.

4. OBSERVANCE

Each Principle should be supported by necessary and sufficient measures (legal, administrative or commercial) to ensure its full observance, and to provide adequate redress for any interferences with privacy resulting from its breach.

5. OPENNESS

There should be a policy of openness about the existence and operation of technologies, administrative systems, services or activities with potential to interfere with privacy.

Openness is needed to facilitate public participation in assessing justifications for technologies, systems or services; to identify purposes of collection; to facilitate access and correction by the individual concerned; and to assist in ensuring the Principles are observed.

6. FREEDOM FROM SURVEILLANCE

People have a right to conduct their affairs free from surveillance or fear of surveillance. 'Surveillance' means the systematic observation or recording of one or more people's behaviour, communications, or personal information.

7. PRIVACY OF COMMUNICATIONS

People who wish to communicate privately, by whatever means, are entitled to respect for privacy, even when communicating in otherwise public places.

8. PRIVATE SPACE

People have a right to private space in which to conduct their personal affairs. This right applies not only in a person's home, but also, to varying degrees, in the workplace, the use of recreational facilities and public places.

9. PHYSICAL PRIVACY

Interferences with a person's privacy such as searches of a person, monitoring of a person's characteristics or behaviour through bodily samples, physical or psychological measurement, are repugnant and require a very high degree of justification.

10. ANONYMOUS TRANSACTIONS

People should have the option of not identifying themselves when entering transactions.

11. COLLECTION LIMITATION

The minimum amount of personal information should be collected, by lawful and fair means, and for a lawful and precise purpose specified at the time of collection. Collection should not be surreptitious. Collection should be from the person concerned, if practicable.

At the time of collection, personal information should be relevant to the purpose of collection, accurate, complete and up-to-date.

12. INFORMATION QUALITY

Personal information should be relevant to each purpose for which it is used or disclosed, and should be accurate, complete and up-to-date at that time.

13. ACCESS & CORRECTION

People should have a right to access personal information about themselves, and to obtain corrections to ensure its information quality.

Organisations should take reasonable measures to make people aware of the existence of personal information held about them, the purposes for which it is held, any legal authority under which it is held, and how it can be accessed and corrected.

14. SECURITY

Personal information should be protected by security safeguards commensurate with its sensitivity, and adequate to ensure compliance with these Principles.

15. USE & DISCLOSURE LIMITATIONS

Personal information should only be used, or disclosed, for the purposes specified at the time of collection, except if used or disclosed for other purposes authorised by law or with the meaningful consent of the person concerned.

16. RETENTION LIMITATION

Personal information should be kept no longer than is necessary for its lawful uses, and should then be destroyed or made anonymous.

17. PUBLIC REGISTERS

Where personal information is collected under legislation and public access is allowed, these Principles still apply except to the extent required for the purpose for which public access is allowed.

18. NO DISADVANTAGE

People should not have to pay in order to exercise their rights of privacy described in this Charter (subject to any justifiable exceptions), nor be denied goods or services or offered them on a less preferential basis. The provision of reasonable facilities for the exercise of privacy rights should be a normal operating cost.