PRB 00-05E

THE PRIVACY OF PERSONAL INFORMATION AND ELECTRONIC COMMERCE — RECENT DEVELOPMENTS

Margaret Smith
Law and Government Division

31 May 2000

PARLIAMENTARY RESEARCH BRANCH
DIRECTION DE LA RECHERCHE PARLEMENTAIRE

The Parliamentary Research Branch of the Library of Parliament works exclusively for Parliament, conducting research and providing information for Committees and Members of the Senate and the House of Commons. This service is extended without partisan bias in such forms as Reports, Background Papers and Issue Reviews. Research Officers in the Branch are also available for personal consultation in their respective fields of expertise.

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

TABLE OF CONTENTS

PAGE

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

THE PRIVACY OF PERSONAL INFORMATION AND ELECTRONIC COMMERCE — RECENT DEVELOPMENTS

INTRODUCTION

Electronic commerce is another name for doing business electronically. This form of commerce covers a diverse range of activities and can be defined broadly or narrowly. Broad definitions include transactions that use digital technology, including open networks such as the Internet and closed networks such as electronic data interchange and debit and credit cards. More narrowly focused definitions, however, limit electronic commerce to transactions using the Internet.(1)

Three types of transactions make up electronic commerce: transactions between businesses, those between businesses and consumers, and government services. To date, most electronic commerce has involved business to business, or business to government transactions and has been conducted over closed systems rather than over the Internet. Indeed, some 80% of electronic commerce transactions are of the business-to-business variety.(2) It is expected that global business-to-business Internet commerce will reach US$2,960 billion by 2003.(3)

Despite the dominant role of business-to-business transactions in the current electronic commerce landscape, it is anticipated that the rapid increase of electronic transactions between businesses and individuals will form the next stage in the development of global electronic commerce. As a result, governments around the world and the private sector are seeking to reduce or eliminate impediments to using the Internet for commercial transactions.

---

(1) Canada, *The Canadian Electronic Commerce Strategy*, 1998, p. 1, http://e-com.ic.gc.ca

(2) *Ibid*., p. 4.

(3) Canada, Task Force on Electronic Commerce, Canadian Internet Commerce Statistics Summary Sheet, 26 August 1999.

Consumers' fear and concern about the confidentiality of their personal information is widely acknowledged as a significant impediment to the development of electronic commerce. Surveys highlight a definite public preference for preserving the privacy of personal information on the Internet. A 1998 Angus Reid survey reported that over 80% of Canadians think personal data should be kept strictly confidential; 65% think it is "not at all acceptable" for companies to sell, trade or share detailed lists of personal information with other organizations; nine in ten Canadians strongly disapprove of companies trafficking in information about their private lives without their consent; and 94% of Canadians feel it is important to have safeguards to protect personal information on the Internet.(4) Although Internet-based electronic commerce is expected to grow significantly, consumer reluctance to conduct business on the Internet is likely to be a concern until issues of security, privacy and redress are satisfactorily resolved.

Technological advances have facilitated the collection of personal information through the Internet. There are many ways to collect such information. First, a Web user can voluntarily supply the information. Second, a user can use software that directly interacts with a Web site; some sites, for example, before they can be used, require a user to download a particular kind of software, thereby revealing his or her identity. Third, individuals may unknowingly volunteer personal information by completing an online questionnaire or registration form in order to gain access to a particular site or to be included in an online directory. Fourth, "cookies" can be used to track and create profiles of Internet users' interests and browsing activities. Cookies are small amounts of computer code placed on a hard drive to track the user's activity on a Web site and use this information when the person next visits the site. The Web site can then tailor online advertising to match the interests of the particular Web user. Though a cookie does not reveal a person's name or e-mail address, it can profile buying habits and store the information in a database. Fifth, tracking software and statistical logs can maintain a record of every Web site and every page on a Web site that has been accessed. Such "clickstream data" (so called because each mouse click is recorded) are often gathered without the knowledge or consent of the consumer.(5)

---

(4) Industry Canada, Office of Consumer Affairs, *Consumer Quarterly*, Vol. 4, No.1, March 1999, p. 2, http://strategis.ic.gc.ca/SSG/ca01129e.html

(5) Dale A. J. Dietrich, *Legal Issues Affecting Canadian Based Electronic Commerce Undertakings*, Paper Presented to IT Industry Series on Intellectual Property, Centre for Property Studies, University of New Brunswick, May 1998, p. 41.

Personal information can be a valuable commodity. Indeed, the collection and use of personal data can be critical to the success of a Web site. Databases that record buying habits, preferences, and demographic particulars can be used to create customized solicitations or sold to other businesses.(6) Thus, the Internet thrives on information but also presents new opportunities to abuse information and invade personal privacy.(7)

Over the past 20 years, governments in the United States, Canada, Australia and Europe have studied how personal information is collected, used and disclosed and the safeguards in place to provide adequate privacy protection. The result has been a series of reports, guidelines, model codes and laws that represent widely accepted principles of fair information practice.

Although fair information practices and privacy initiatives are relevant to both the public and private sectors, this paper focuses on initiatives to protect the privacy of personal information in the private sector in the context of electronic commerce. Efforts by governments in Canada, the United States, United Kingdom and Australia, as well as industry self-regulatory initiatives, will be discussed.

PRINCIPLES OF FAIR INFORMATION PRACTICE

Many of the initiatives to protect the privacy of personal information are based on five key privacy protection principles. These are listed and explained below.

1. Notice/Awareness
2. Choice/Consent
3. Access/Participation
4. Integrity/Security
5. Enforcement/Redress.(8)

---

(6) Ann Cavoukian, Information and Privacy Commissioner/Ontario, *Privacy: The Key to Electronic Commerce*, April 1998, p. 4.

(7) Dietrich, *Legal Issues Affecting Canadian Based Electronic Commerce Undertakings*, 1998, p. 40.

(8) United States, Federal Trade Commission, *Privacy Online: A Report to Congress*, June 1998, p. 10, http://www.ftc.gov/reports/privacy3/fairinfo.htm

1. Notice/Awareness

The principle of notice requires that consumers be given notice of an entity's information practices before any personal information is collected from them; in this way they can make an informed decision as to whether to disclose their personal information and to what extent. Such notice includes:

- identifying who is collecting the information;
- identifying how the information will be used;
- identifying potential recipients of the information;
- indicating the type of information collected and how it is collected, if this is not obvious;
- whether providing the information is mandatory or voluntary and the consequences of not providing it; and
- what the entity collecting the information has done to ensure the confidentiality, integrity and quality of the information.(9)

2. Choice/Consent

Another principle of fair information practice is consumer choice or consent. This involves giving consumers options in relation to how their personal information is to be used. This is particularly relevant to secondary uses of the information that are over and above those necessary to complete the contemplated transaction.(10)

There are typically two kinds of choice schemes -- opt-in and opt-out. Opt-in schemes require the individual's consent before the collection, use or disclosure of personal information can take place while opt-out schemes assume that the information can be collected, used or disclosed unless the individual takes steps to prevent this from happening.

3. Access/Participation

The third essential principle -- access -- refers to a person's ability to have access to his or her own information and to ensure that the information is accurate and complete.(11)

---

(9) *Ibid*., p. 7.

(10) *Ibid*., p. 8.

(11) *Ibid*.

4. Integrity/Security

This principle requires that data be accurate and secure. This involves instituting both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the information. Managerial measures include internal organizational measures that limit access to the information and ensure that persons having such access do not use the information for unauthorized purposes. Technical security measures include encryption in the transmission and storage of data, limits on access through use of passwords, and the storage of data on secure servers or computers that are inaccessible by modem.(12)

5. Enforcement/Redress

Effective enforcement mechanisms are essential to protect privacy. There are several approaches to enforcement including industry self-regulation, legislation creating private remedies for consumers, or some type of regulatory scheme enforceable through civil and criminal sanctions.(13)

INTERNATIONAL DEVELOPMENTS IN RELATION TO PRIVACY PROTECTION

A. OECD -- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

One of the first multinational efforts to establish guidelines for the protection of personal information was undertaken by the Organisation for Economic Co-operation and Development (OECD). In 1980, the OECD adopted a number of privacy principles relating to personal information in the public or private sectors. Representing a consensus among OECD member countries, these principles were set out in Guidelines on the Protection of Privacy and

(12) *Ibid*., p. 9.

(13) *Ibid*., p. 10-11.

Transborder Flows of Personal Data.[14] The Guidelines contained the following eight privacy principles:

Collection limitation principle: There should be limits to the collection of personal information, which should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

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

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

Use limitation principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the purpose specification principle] except with the consent of the data subject or by the authority of law.

Security safeguards principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and the usual residence of the data controller.

Individual participation principle: Individuals should have the right:

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

(b) to have communicated to them, data relating to them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to them;

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

(14) Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

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

Accountability principle: A data controller should be accountable for complying with measures that give effect to the principles stated above.

Although the OECD Guidelines are voluntary and have no force in law, they have served as the foundation of privacy protection schemes in a number of countries. They have not, however, produced the harmonization of data protection regimes that was hoped for.(15)

B. European Union -- Directive on the Protection of Personal Data with Regard to the Processing of Personal Information and on the Free Movement of Such Data

In 1995, the European Union Council of Ministers adopted the Directive on the Protection of Personal Data with Regard to the Processing of Personal Information and on the Free Movement of Such Data.(16) Members of the European Union were required to bring the Directive into effect in their States by 24 October 1998.

The Directive has two purposes: to protect individuals in relation to the processing of their personal data and to provide for the free flow of personal data between Member States through the harmonization of national data protection laws.

The EU Directive contains a number of data quality principles. Member States must ensure that personal data are:

- processed fairly and lawfully;
- collected and processed for specified, explicit and legitimate purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected;
- accurate and kept up-to-date; and
- kept for no longer than is necessary.(17)

---

(15) Tom Wright, *Privacy Protection Models for the Private Sector*, Information and Privacy Commissioner of Ontario, 1996, p. 4.

(16) European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal L 281, 23/11/1995, p. 0031-0050.

(17) EU Directive, Article 6.

In addition, subject to several exceptions, personal data can be processed only if the data subject has unambiguously consented to this. These exceptions include processing necessary for the performance of contractual obligations or certain legal obligations and the protection of vital or legitimate interests of either the data subject or the data controller.(18)

Again, subject to certain exceptions, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership is prohibited, as is the processing of data concerning an individual's health or sex life.(19)

The EU Directive gives a number of rights to individuals about whom personal data are collected: the individual must be informed of the identity of the data controller, the purposes for which the data are collected, the recipients of the data and the right to access and correct the data.(20) Where the data have not been obtained directly from the data subject, the controller must provide him or her with the same information unless (and particularly in processing for statistical purposes or for historical or scientific research) this would prove impossible or would involve a disproportionate effort.(21)

The EU Directive provides that a data subject has the right to object to the processing of personal data for direct marketing purposes.(22) The Directive also provides that individuals have the right to a judicial remedy for any breach of the rights and to compensation.(23)

Each Member State must appoint an independent supervisory authority to monitor and enforce the application of the EU Directive. The supervisory authority is to have investigative powers, powers of intervention and the power to engage in legal proceedings for violations of national data protection legislation adopted pursuant to the EU Directive.(24)

---

(18) *Ibid*., Article 7.

(19) *Ibid*., Article 8.

(20) *Ibid*., Article 10.

(21) *Ibid*., Article 11.

(22) *Ibid*., Article 14.

(23) *Ibid*., Articles 22 and 23.

(24) *Ibid*., Article 28.

The EU Directive also provides for codes of conduct drawn up by trade associations and other bodies.(25)

Article 25 of the EU Directive deals with the transfer of personal data from EU Member States to third countries. Such transfers are permitted only if the third country ensures "an adequate level of protection" for such data. What constitutes an "adequate level of protection" is an important issue for non-EU members. The Directive notes that the adequacy of the level of protection provided by a third country is to be assessed in light of all the circumstances surrounding a data transfer operation, with particular consideration given to the nature of the data; the purpose and duration of the proposed processing operation; the country of origin and the country of final destination; the rules of law, both general and sectoral, in force in the third country; and the professional rules and security measures that are complied with in that country.(26)

Where the Commission finds that a third country does not ensure an adequate level of protection, Member States are to prevent the transfer of data to that country. The Directive does go on, however, to provide that the transfer of data to a third country without adequate protection may still take place on condition that:

- the data subject has unambiguously consented to the proposed transfer;
- the transfer is necessary for the performance of a contract between the data subject and controller or a contract between the controller and a third party in the interest of the data subject;
- the transfer is legally required on important public interest grounds or for the exercise, establishment or defence of legal claims;
- the transfer is necessary to protect the vital interests of the data subject; or
- the transfer is made from a register of information that is open to the public in general or to anyone with a legitimate interest.(27)

Personal data can also be transferred to a third country that does not ensure an adequate level of protection where the data controller "adduces adequate safeguards with respect

(25) *Ibid*., Article 27.

(26) *Ibid*., Article 25 (2).

(27) *Ibid*., Article 26(1).

to the protection of privacy and fundamental rights and freedoms of individuals as regards the exercise of corresponding rights; such safeguards may in particular result from appropriate contractual clauses."(28)

On another front, the European Commission has proposed the creation of a "dot-EU" high-level Internet domain name with a privacy policy to which all sites would be required to adhere in order to register. It is hoped that a guarantee of strict privacy measures would increase consumers' confidence in the use of the Internet and give companies registered on the site a marketing advantage over those with less rigorous privacy standards.

C. Council of Europe -- Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on Information Highways Which May Be Incorporated in or Annexed to Codes of Conduct

On 23 February 1999, the Committee of Ministers of the Member States of the Council of Europe adopted Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on Information Highways. These guidelines set out principles relating to fair privacy practice for Internet users and Internet service providers (ISPs). The Council suggests that these guidelines be incorporated into ISP codes of conduct. Internet service providers, for example, should:

- inform users of privacy risks presented by use of the Internet before they subscribe;
- inform users about technical means that they may lawfully use to reduce security risks to data and communications;
- not interfere with the contents of communications unless the law so provides;
- not communicate data unless such communication is permitted by law; and
- not use data for promotional or marketing purposes.(29)

---

(28) *Ibid*., Article 26(2).

(29) Council of Europe, Committee of Ministers, Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on Information Highways, Rec. No. R(99)5, 23 February 1999, p. 4, http://www.coe.fr/cm/ta/rec/1999/99r5.htm

D. OECD Ministers -- Declaration on the Protection of Privacy on Global Networks

At their 1998 Ottawa Conference, "A Borderless World: Realising the Potential of Global Electronic Commerce," the OECD Ministers released a Declaration on the Protection of Privacy on Global Networks. In this, the Ministers confirmed their commitment to the protection of privacy on global networks and agreed to take the necessary steps to ensure that the OECD Privacy Guidelines are effectively implemented in relation to global networks, and in particular to:

- encourage the adoption of privacy policies, whether implemented by legal, self-regulatory, administrative or technological means;
- encourage the online communication of privacy policies to users;
- ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress;
- promote users' education and awareness about online privacy issues and the means at their disposal for protecting privacy on global networks;
- encourage the use of privacy-enhancing technologies; and
- encourage the use of contractual solutions and the development of model contractual solutions for online transborder data flows.(30)

E. Privacy Initiatives in the United States

Unlike the European Union and Canada, the United States favours a non-legislative approach to protecting privacy on the Internet. As a result, the Administration has consistently promoted private sector self-regulatory initiatives, although it has indicated that it would reevaluate its preference for self-regulation if effective privacy protection could not be achieved that way.

This strategy was set out in the July 1997 White House document *A Framework for Global Electronic Commerce* (the "Framework"), which established the following principles to facilitate the growth of electronic commerce in the U.S.:

---

(30) Organisation for Economic Co-operation and Development, Declaration on the Protection of Privacy on Global Networks, SG/EC(98)14/Final, October 1998, p. 2.

- The private sector should lead.
- Governments should avoid undue restrictions on electronic commerce.
- Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.
- Governments should recognize the unique qualities of the Internet.
- Electronic commerce over the Internet should be facilitated on a global basis.(31)

The Framework sets out nine areas where international agreements would be needed to "preserve the Internet as a non-regulatory medium." These areas were grouped into three main categories: financial issues, legal issues, and market access issues. The legal issues included a Uniform Commercial Code for electronic commerce, intellectual property protection, privacy and security.(32)

The *Presidential Directive on Electronic Commerce* (1 July 1997) was designed to implement the strategy set out in the Framework. The Directive gave 13 specific tasks to various Cabinet agencies. One of these was for the Secretary of Commerce and the Director of the Office of Management and Budget to "encourage private industry and privacy advocacy groups to develop and adopt within the next 12 months effective codes of conduct, industry developed rules, and technological solutions to protect privacy on the Internet..."(33)

On the privacy front then, the goal was to promote self-regulation and thereby avoid the need for regulatory or legislative initiatives. Following upon this, in June 1998 the U.S. Federal Trade Commission released a report to Congress on the results of its examination of the privacy practices of over 1,400 commercial Web sites; these had been assessed for their conformity with core principles of fair information practices. The survey revealed that adherence to privacy protection principles by many Web sites fell short of acceptable standards. While nearly 85% of the Web sites surveyed collected information from consumers, only 14%

(31) United States, Executive Office of the President, *A Framework for Global Electronic Commerce*, 1 July 1997, p. 2-3.

(32) *Ibid*., p. 3-4.

(33) United States, U.S. Government Working Group on Electronic Commerce, *First Annual Report*, November 1998, p. 15-16.

provided notice of their information practices and only 2% had a comprehensive privacy policy. Of Web sites aimed at children, the Commission found that 89% collected personal information from children but only 23% of those sites told children to obtain parental permission before providing it and even fewer allowed for parental control over the collection and use of information obtained from children.(34)

The FTC expressed its continuing commitment to self-regulatory measures to protect the privacy of personal information on the Internet but noted that, despite its urgings and privacy initiatives, effective self-regulatory regimes had not yet been implemented. The Commission called for more incentives to spur self-regulation and ensure the widespread implementation of basic privacy principles.

> The Commission has encouraged industry to address consumer concerns regarding online privacy through self-regulation. The Internet is a rapidly changing marketplace. Effective self-regulation remains desirable because it allows firms to respond quickly to technological changes and employ new technologies to protect consumer privacy. Accordingly, a private-sector response to consumer concerns that incorporates widely-accepted fair information practices and provides for effective enforcement mechanisms could afford consumers adequate privacy protection. To date, however, the Commission has not seen an effective self-regulatory system emerge.
>
> As evidenced by the Commission's survey results, and despite the Commission's three-year privacy initiative supporting a self-regulatory response to consumers' privacy concerns, the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness). Moreover, the trade association guidelines submitted to the Commission do not reflect industry acceptance of the basic fair information practice principles. In addition, the guidelines, with limited exception, contain none of the enforcement mechanisms needed for an effective self-regulatory regime.(35)

The Commission recommended, however, that Congress develop legislation placing parents in control of the online collection and use of personal information from their children and setting out basic standards of practice governing this. All commercial Web sites

---

(34) United States Federal Trade Commission, *Privacy Online: A Report to Congress*, 1998, p. 2.

(35) *Ibid*., p. 24-25.

directed to children would be required to comply with these standards.(36) Following the recommendations of the FTC, in 1998, the *Children's Online Privacy Protection Act of 1998* (COPPA) was signed into law. In the fall of 1999, the FTC issued its final rule implementing the COPPA, which will come into effect on 21 April 2000.

The COPPA and the FTC rule apply to commercial Web sites directed to children under 13, limiting the information collected to what is necessary for a child's participation in an activity. The Act requires the operator of the Web site to post a clear and prominent privacy policy and to obtain verifiable parental consent prior to collecting, using or disclosing personal information from a child. The statute also includes a "safe harbor" program for industry groups or others who wish to create self-regulatory programs to govern participants' compliance. Under the law, the FTC is authorized to bring enforcement actions and impose civil penalties for violations of the rule.(37)

A more recent government report paints a rosier picture of the state of self-regulatory privacy initiatives. The 1999 report of the U.S. Government Working Group on Electronic Commerce, *Towards Digital eQuality*, noted that privacy policies have become more common on private sector Web sites and self-regulatory efforts widespread and enforceable.(38) According to the report, the private sector claims that nearly two-thirds of commercial Web sites now post privacy policies or information practice statements, an increase from 14% the year before.(39) The report reiterated the U.S. government's commitment to self-regulation and went on to note that the government will continue to monitor the progress of self-regulation to establish whether such programs actually protect the privacy of Internet users. This will include an online survey by the FTC in 2000 to reassess the progress in implementing fair information practices.

Another report was issued in December 1999 by the Electronic Privacy Information Center (EPIC), a U.S. civil liberties group that focuses on internet privacy, encryption, information access and other related issues. This was less sanguine about privacy

---

(36) *Ibid*., p. 25.

(37) United States Federal Trade Commission, Press Release, New Rule Will Protect Privacy Online, 20 October 1999, http://www.ftc.gov/opa/1999/9910/childfinal.htm

(38) U.S. Government Working Group on Electronic Commerce, *Towards Digital eQuality*, 2nd Annual Report, 1999, p. 35.

(39) *Ibid*., p. 35-36.

practices on the Internet.(40) EPIC reviewed the privacy practices and policies of the 100 most popular shopping Web sites to see if they were in compliance with "Fair Information Practices" principles, and whether they used profile-based advertising and cookies. EPIC found that all 100 sites collected personally identifiable information but none required users to disclose personal information when entering or browsing. While 51 sites provided a link to their privacy policies on their homepage, 18 sites had no privacy policy. EPIC also noted that 20 sites belonged to an industry self-regulation program, such as TRUSTe or the Better Business Bureau Online.(41)

EPIC noted a wide variation in the privacy policies of the 100 sites. More sites were posting privacy policies and new associations had been formed to promote the development of such policies and to encourage industry awareness of privacy issues; however, most policies typically "lacked the necessary elements of Fair Information Practices and were unlikely to provide meaningful privacy protection for consumers."(42)

Another study issued a few months prior to the EPIC review examined the extent to which commercial Web sites have posted privacy disclosures based on fair information practices.(43) The Georgetown Internet Privacy Policy Survey sampled 361 .com Web sites visited by consumers at home that were drawn from the top 7500 URL's ranked by audience during January 1999. The study addressed the following three questions:

1. What personal information do Web sites collect from consumers?
2. How many Web sites posted privacy disclosures?
3. Do these disclosures reflect fair information practices?

In response to the first question, the survey revealed that 92.8% of the sites in the sample collected at least one type of personal identifying information (e.g., name, e-mail address, and postal address). At least one type of demographic information (e.g., gender, preferences, Zip

---

(40) Electronic Privacy Information Center, Surfer Beware III: Privacy Policies without Privacy Protection, December 1999, http://www.epic.org/reports/surfer-beware3.html

(41) *Ibid*., p. 3-4.

(42) *Ibid*., p. 6.

(43) Georgetown Internet Privacy Policy Survey: Final Report, June 1999. This study was initiated by the private sector and funded by contributions from 17 companies and organizations, http://www.msb.georgetown.edu/faculty/culnanm/gippshome.html

code) was collected by 56.8%; 56.2% of the sites collected both personal identifying and demographic information and 6.6% of the sites collected neither type of personal information.(44)

The study found that 65.3% (236) of the 361 sites had posted at least one type of privacy disclosure (a privacy policy notice or an information practice statement); 36% (131 sites) had posted both types of disclosures while 34.1% (123 sites) had not posted either type of privacy disclosure.(45)

To determine whether these disclosures reflect fair information practices, the content of all privacy disclosures were analyzed for four elements of fair information (notice, choice, access and security) and whether they posted information on where to ask questions or make complaints about privacy issues. Of the 236 Web sites that collected personal information and posted a privacy disclosure, 89.8% included at least one survey item for notice, 61.9% contained at least one survey item for choice, 40.3% contained at least one survey item for access, 45.8% contained at least one survey item for security, and 48.7% contained at least one survey item for contact information.(46)

The report did not draw any conclusions or make any policy recommendations about the effectiveness of self-regulation as a means of protecting privacy on the Internet.

---

(44) *Ibid*., p. 1.

(45) *Ibid*.

(46) *Ibid*. The contents of privacy disclosures were analyzed to determine if they included notice, choice, access or security.

These four elements of fair information practices were operationalized as follows:

- Notice was defined to include statements about what information is collected, how the information is collected, how the information collected will be used, whether the information will be reused or disclosed to third parties, and whether the site said anything about its use or non-use of cookies.
- Choice was defined to include statements regarding choice offered about being contacted again by the same organization and choice about having non-aggregate personal information collected by the Web site disclosed to third parties.
- Access was defined to include allowing consumers to review or ask questions about the information the site had collected and whether the sites disclosed how inaccuracies in personal information the site had collected were handled.
- Security was defined to include protecting information during transmission and during subsequent storage.

The privacy disclosures were further analyzed to see if they provided information a consumer could use to contact the company to ask a question about the site's information practices or to complain to the company or another organization about invasion of privacy.

Based in part on the results of the Georgetown Internet Privacy Study, a majority of the U.S. Federal Trade Commission recommended in the 1999 report to Congress, *Self-Regulation and Privacy Online*,(47) that self-regulation be given more time to develop. At the same time, the report called for industry to do more to implement fair information practice principles.

In February and March 2000, the FTC once again surveyed the information practices of commercial Web sites. The 2000 online survey results set out in the May 2000 report to Congress *Privacy Online: Fair Information Practices in the Electronic Marketplace*(48) reviewed the nature and substance of privacy disclosure on U.S. commercial Web sites and assessed the effectiveness of self-regulation as a means of protecting consumer privacy online.

While the FTC applauded the development of industry self-regulatory initiatives, the majority of the Commission took the position that industry efforts alone had not been sufficient and could not ensure that the online marketplace as a whole would follow the standards adopted by industry leaders.(49) The Commission noted that only 20% of the busiest Web sites had to any extent implemented all four fair information practices in their privacy disclosures and that fewer than half of the sites surveyed (41%) met the relevant standards with respect to Notice and Choice. In addition, only 8% of the busiest Web sites displayed a seal from one of the self-regulatory seal programs.(50)

In a change of direction from its previous reports, a majority of the FTC went on to recommend that Congress enact legislation to ensure adequate protection of consumer privacy online. The majority recognized, however, that industry self-regulation would still play an important role in a legislative structure.(51)

The self-regulatory approach to protecting privacy on the Internet has important ramifications for trade relations between the European Union and the United States. While the European Union has established a legislative/regulatory framework, the United States, except in the areas of online privacy relating to children, has promoted self-regulation over legislation. The

---

(47) United States Federal Trade Commission, *Self-Regulation and Privacy Online*, July 1999.

(48) United States Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, May 2000.

(49) *Ibid*., p. 35.

(50) *Ibid*.

European Union Directive on Data Protection prohibits the exchange of personal data with countries that do not meet adequate privacy standards.

Because the U.S. has not enacted comprehensive data protection legislation governing the private sector, there is considerable uncertainty about whether non-legislative solutions to privacy protection are adequate for the purposes of the Data Protection Directive of the EU. In an effort to reduce this uncertainty, the U.S. Department of Commerce has developed "International Safe Harbor Privacy Principles." These principles, which are intended for use by U.S. organizations receiving personal data from the European Union, aim to satisfy the adequacy requirements of Article 25 of the EU Directive. Decisions by U.S. organizations to qualify for the safe harbour are voluntary. Organizations that decide to adhere to the principles, however, must comply with them in order to obtain the benefits of the safe harbour. The Safe Harbor Privacy Principles continue to be the subject of negotiation with the EU. A preliminary agreement that would allow for the uninterrupted flow of information between Europe and the U.S. is reported to have been reached in late February 2000; it is anticipated that an agreement will finalized by the end of March 2000.(52)

F. Privacy Initiatives in Australia

After extensive consultation with business and consumers, in February 1998 the Australian Privacy Commissioner issued the National Principles for the Fair Handling of Personal Information (National Principles). These were designed to provide a framework within which business could develop practices to protect the privacy of individuals. Following additional consultation, the National Principles were revised in January 1999.

In December 1998, the Australian federal government announced that it would develop "light touch" legislation to support and strengthen self-regulatory privacy protection initiatives in the private sector.(53) At the present time, there is no general legislation in Australia that regulates the handling of personal information in the private sector, although credit providers

---

(cont'd)

(51) *Ibid*., p. 36-37.

(52) John Burgess, "Accord Near on Data Privacy," *Washington Post*, 24 February 2000, p. A12.

(53) Australia, Attorney General's Department, Information Paper, The government's proposed legislation for the protection of privacy in the private sector, September 1999, p. 3. http://law.gov.au/infopaper/infopaper.html

and credit reporting agencies are regulated in relation to reporting information with respect to personal credit.

In 1999, the government released draft key provisions of its proposed privacy scheme for the private sector. The draft provisions would recognize self-regulatory privacy codes that would be backed by a default legislative scheme and complaint-handling regime that would apply where no privacy codes were in place. This scheme would appear to be a middle ground between the legislative/regulatory approach of the European Union and the self-regulatory approach adopted in the United States.

The proposed legislation would contain National Privacy Principles (NPPs) applying to the acts and practices of an organization, which could be an incorporated body, a partnership, an unincorporated body, a charitable organization, a community organization or an individual if he or she were a sole proprietor.(54)

Not all personal information held by the private sector, however, would be subject to the legislation. Exemptions would be given to:

- personal information collected and used in a domestic capacity;
- employee records;
- personal information collected, used and disclosed by the media for the purpose of informing the public;
- State or Territory public sector agencies; and
- small business.(55)

The proposals would exempt a small business organization (a business with an annual turnover of $1,000,000 or less) where there was a low privacy risk. A small business organization would be defined as an organization that carried on a small business, did not hold any sensitive information and did not transfer personal information about an individual to another person for a benefit, service or advantage.(56)

---

(54) *Ibid*., p. 11.

(55) *Ibid*., p. 11-12.

(56) Australia, Attorney General's Department, "Overview of Key Provisions of Privacy Amendment (Private Sector) Bill," 20 December 1999, p. 3-4, http://law.gov.au/privacy/overview.html

The proposed draft provisions would set out NPPs for the private sector and allow a privacy code to include its own Code Privacy Principles (CPPs) which would replace or incorporate all the NPPs, and provide at least the same level of protection. The CPPs would apply to private sector organizations that agreed to be bound by a particular approved code.(57)

The NPPs cover the following:

Collection: Among other things, this principle provides that only information that is necessary for the operations of an organization should be collected. Collection should lawful and fair. At the time the information is collected, the intended uses of the information should be made clear.

Use and Disclosure: This principle limits use and disclosure of information to the primary purpose for which it has been collected. Use or disclosure for a secondary purpose is permitted in specified circumstances, including where the individual consents, and where the secondary purpose is related and is within the reasonable expectation of the individual.

Data Quality: This principle requires organizations to ensure that the information collected is accurate, complete and up-to-date.

Data Security: This requires organizations to ensure that any personal information they hold is kept secure.

Openness: Organizations must be open about the kinds of personal information they hold and what they do with it.

Access and Correction: Wherever possible, organizations should allow individuals to see the personal information that is held about them and to correct any inaccuracies.

Identifiers: This principle would discourage private sector organizations from using as their own identifier for an individual, the same identifier assigned to that individual by a government agency.

Anonymity: Individuals, in many circumstances, should be able to remain anonymous when dealing with private sector organizations.

Transborder Data Flows: This principle would establish the conditions under which an organization would be able to transfer personal information to someone in a foreign country. For example, the foreign recipient of the information must be subject to a law, binding scheme or contract that protects the privacy of such information or the individual must consent to the transfer.

---

(57) Australia, “Proposed Legislation for the Protection of Privacy in the Private Sector,” September 1999, p. 13.

Sensitive Information: This principle would limit the collection of sensitive information about individuals, such as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or details of health or sex life.(58)

The proposed draft goes into considerable detail about the development of private sector privacy codes. An approved code would apply to the activities of an organization and thereby override the default legislative NPPs; if the code provided for complaint handling, the legislative complaint mechanisms would also be overridden. The Privacy Commissioner would have responsibility for approving privacy codes as well as variations to approved codes. The Commissioner would also be able to revoke approval of a privacy code.

Before a code could receive approval, among other things it would have to:

(a) incorporate all the National Privacy Principles or set out obligations that were at least the equivalent of all the obligations set out in the Principles;

(b) specify the organizations bound by the code or a way of determining the organizations that were, or would be, bound by the code;

(c) provide that only organizations that consented to be bound by the code were, or would be, so bound;

(d) provide that the code would set out a procedure whereby an organization might cease to be bound by the code and when the cessation would take effect;

(e) provide that members of the public had been given an adequate opportunity to comment on a draft of the code;

(f) meet prescribed standards and the Commissioner's guidelines for dealing with complaints if a code had a complaint-handling process;

(g) have an independent adjudicator; and

(h) provide for an annual report on the operation of the code.

The Australian Government intends to introduce its privacy bill in 2000. It is expected that the legislation will become fully effective on 1 July 2001.(59)

(58) *Ibid*., p. 13-14.

(59) *Ibid*., p. 10.

G. Privacy Initiatives in the United Kingdom

As a member of the European Union, the United Kingdom was required to implement the 1995 EU Data Protection Directive. The *Data Protection Act 1998*(60) (the "Act") gives effect in UK law to the Directive. The Act, which amends the *Data Protection Act 1984*, received Royal Assent on 16th July 1998 and came into force on 1 March 2000. The Act applies to data controllers who are established in the United Kingdom or who use equipment in the UK for processing data. It follows a notification system for data protection whereby persons wishing to process data must notify the Data Protection Commissioner. The Act also gives legal rights to individuals (data subjects) in respect of personal data held about them by others.

The Act contains a number of definitions of important terms. Among these are: "personal data," "sensitive personal data," "data subject," "data controller" and "processing." The term "personal data" means:

> data that relate to a living individual who can be identified
>
> (a) from those data, or
> (b) from those data and other information which is in the possession of or is likely to come into the possession of, the data controller,
>
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.(61)

The Act also introduces a new category of "sensitive personal data" that is subject to additional safeguards. Sensitive personal data includes information on

- racial or ethnic origin;
- political opinions, religious or similar beliefs;
- trade union membership;
- physical or mental health;

---

(60) *Data Protection Act 1998*, U. K. Statutes 1998 Chapter 29, http://www.hmso.gov.uk/acts/acts1998/19980029.htm

(61) *Ibid*., section 1(1).

- sexual life; and
- the commission of any offence, subsequent proceedings or sentence.(62)

For the purposes of the Act, a "data subject" is an individual who is the subject of personal data, while a "data controller" is a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed. The term "processing" is broadly defined; it refers to obtaining, recording, holding, adapting, using, disclosing, destroying or blocking information or data.(63)

The Act also sets out eight Data Protection Principles that cover how personal data must be processed:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specified conditions are met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under the Act.

7. Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.(64)

---

(62) *Ibid*., section 2.

(63) *Ibid*.

(64) *Ibid*., Schedule I, Part I.

Unless an exemption exists, at least one of the following conditions must be met for the processing of personal data:

- the consent of the data subject must have been obtained;
- the processing must be necessary for:
  (i) performing a contract to which the data subject is a party, or
  (ii) taking steps at the request of the data subject to enter into a contract;
- the processing must be necessary to comply with any legal obligation to which the data controller is subject, other than being an obligation imposed by contract;
- the processing must be necessary for protecting the vital interests of the data subject;
- the processing must be necessary for:
  (i) the administration of justice,
  (ii) the exercise of any functions conferred by or under any enactment,
  (iii) the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
  (iv) the exercise of any other functions of a public nature exercised in the public interest;
- the processing must be necessary for legitimate interests pursued by the data controller or by others to whom the data are disclosed, except where the processing is unwarranted because of prejudice to the rights and freedoms or legitimate interests of the data subject.(65)

Sensitive personal data must not be processed unless at least one of the above listed conditions and at least one of the conditions set out in Schedule 3 to the Act have been satisfied. The explicit consent of the individual will usually be required before sensitive personal data can be processed unless the data controller can demonstrate that the processing is necessary because of one of the other criteria set out in Schedule 3.(66)

---

(65) *Ibid*., Schedule 2.

(66) Schedule 3 provides as follows:

- there must be the explicit consent of the data subject.
- the processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
- the processing is necessary:

  a) in order to protect the vital interests of the data subject or another person, in a case where:

  (i) consent cannot be given by or on behalf of the data subject, or

(cont'd)

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

b) to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

- the processing:

  a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade-union purposes and which is not established or conducted for profit,

  b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

  c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes, and

  d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

- the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

- the processing:

  a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

  b) is necessary for the purpose of obtaining legal advice, or

  c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

- the processing is necessary for:

  a) the administration of justice,

  b) the exercise of any functions conferred by or under any enactment, or

  c) the exercise of any functions of the Crown, a Minister of the Crown or a government department.

- the processing is necessary for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by:

  a) a health professional (as defined in the Act), or

  b) a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

- the processing:

  a) is of sensitive personal data consisting of information as to racial or ethnic origin,

  b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

  c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

The Act also gives rights to individuals in respect of their personal data. These include:

- the right to have access to the data (sections 7 to 9);
- the right to prevent processing likely to cause damage or distress (section 10);
- the right to prevent processing for the purposes of direct marketing (section 11);
- rights in relation to automated decision-taking (section 12);
- the right to take action for compensation if the individual suffers damage by any contravention of the Act by a data controller (section 13);
- the right to take action to rectify, block, erase or destroy inaccurate data (section 14); and
- the right to make a request to the Data Protection Commissioner for an assessment to be made as to whether any provision of the Act has been contravened (section 42).

Subject to certain exceptions, data controllers are required to notify the Commissioner before they begin processing personal data. The Act establishes broad categories of information about which notification must be given, including the name and address of the data controller, a description of the personal data to be processed, as well as the categories of data subject to which they relate, a description of the persons to whom the data controller intends to disclose the data, countries outside the EU to which the data will be transferred and a description of the purposes for which the data are being processed.(67)

The Act contains a number of exemptions, which are found in the various provisions of Part IV (sections 28-38) and Schedule 7.

Exemptions exist for national security purposes(68) and for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection taxes.(69) In addition, under section 30 of the Act, the Secretary of State may also exempt personal data relating to an individual's physical or mental health or condition as well as other kinds of data.

---

(67) *Ibid*., section 16.

(68) *Ibid*., section 28.

(69) *Ibid*., section 29.

The Act contains exemptions for journalistic, artistic and literary purposes, provided certain conditions are met,(70) and in respect of the processing of personal data for research purposes (including statistical or historical purposes). Exemptions also exist for data that a data controller is required by law to make available to the public.(71)

Exemptions from the non-disclosure provisions of the Act exist where the disclosure is required by law or by court order or in connection with obtaining legal advice or engaging in legal proceedings.(72) An exemption for domestic purposes is available where an individual processes personal data in relation to his or her personal, family or household affairs.(73)

The Act establishes the office of The Data Protection Commissioner, an independent officer reporting directly to Parliament.

The duties of the Commissioner include:

- promoting good practice by data controllers and the observance of the requirements of the Act;
- spreading information about the Act and how it works;
- after consultation with stakeholders, preparing codes of practice for guidance as to good practice in processing personal data;
- encouraging trade associations to develop codes of practice;
- examining codes of practice prepared by trade associations;(74)
- reporting annually to Parliament;(75) and
- assessing requests as to whether the processing of personal data complies with the Act.

(70) *Ibid*., section 32.

(71) *Ibid*., section 34.

(72) *Ibid*., section 35.

(73) *Ibid*., section 36.

(74) *Ibid*., section 51.

(75) *Ibid*., section 52.

The Act also confers enforcement powers on the Commissioner. Through enforcement notices, the Commissioner can require a data controller to take, or refrain from taking, specified steps or to refrain from processing any personal data altogether. Failure to comply with an enforcement notice is an offence unless the person charged is able to show that he or she exercised due diligence to comply with the notice. There is a right of appeal to the Data Protection Tribunal against an enforcement notice.

Among other things, the Act enables the Commissioner to provide assistance in appropriate cases to individuals who are a party to proceedings relating to specified provisions of the Act. Although the Commissioner has considerable discretion in this regard, assistance may be given only where the Commissioner believes that the case involves a "matter of substantial public importance."(76)

The Act confers powers of entry and inspection on the Commissioner. If there are reasonable grounds for suspecting that an offence has been or is being committed under the Act or that any of the Data Protection Principles have been or are being contravened, the Commissioner may apply for a warrant to enter and search a premises.

There are a number of offences set out in the Act, including:

- processing data without notification;
- failure to comply with an enforcement notice/information notice;
- knowingly or recklessly making a false statement in compliance with an information notice;
- intentional obstruction of, or failure to give reasonable assistance in, execution of a warrant;
- without the consent of the data controller, to knowingly or recklessly:
  (i) obtain or disclose personal data or the information contained in personal data, or
  (ii) procure the disclosure to another person of the information contained in personal data;
- unlawfully selling personal data; and
- the unlawful disclosure of information by the Commissioner.(77)

(76) *Ibid*., section 53.

(77) *Ibid*., section 55.

The Act imposes personal liability for any of the offences on directors or other officers of a corporation that has committed an offence. Where a company commits the offence with the consent or connivance of, or due to any neglect on the part of, the director or officer concerned, that person will be guilty of the offence.(78)

H. Privacy Initiatives in Canada

The development of standards to protect the confidentiality of information in the private sector in Canada largely began when the federal government affirmed its commitment to the OECD Guidelines in 1984. At that time the federal government sought to encourage the private sector to develop and adopt voluntary privacy protection codes.(79) By the end of the 1980s, however, the federal Privacy Commissioner was concerned about the lack of progress in this regard and called for federal legislation requiring federally regulated corporations to develop such codes.(80)

Recognizing the potential of electronic commerce, in the latter half of the 1990s the government began developing strategies and policies to deal with the various business, legal, technological and social issues arising from it.

In 1996, Industry Canada's report *Building the Information Society* stated that the right to privacy must be recognized in law, especially in situations where personal information about individuals is collected in electronic databases.(81) In that same year, the federal Ministers of Industry and Justice announced that the federal government would legislate to protect privacy.

In January 1998, Industry Canada and the Department of Justice released a discussion paper, *The Protection of Personal Information*, in which it was noted that ensuring consumer confidence was essential to the growth of the information economy. The Paper observed that "legislation that establishes a set of common rules for the protection of personal information will help to build consumer confidence and create a level playing field [so that] the

---

(78) *Ibid*., section 61.

(79) Privacy Commissioner of Canada, *Annual Report 1984-85*, Ottawa, Supply and Services Canada, 1985.

(80) Privacy Commissioner of Canada, *Annual Report 1988-89*, Ottawa, Supply and Services Canada 1989; *Annual Report 1989-90*, Ottawa, Supply and Services Canada, 1990.

(81) Canada, Department of Industry, *Building the Information Society: Moving Canada into the 21st Century*, Ottawa, 1996, p. 25.

misuse of personal information cannot result in a competitive advantage."[82] Federal privacy legislation, the Paper noted, would have to address the following four key elements:

- obligations based on fair information practices;
- administrative arrangements for an overseeing body to ensure accountability;
- powers for overseeing authorities and judicial bodies; and
- powers and responsibilities that will promote public awareness and ensure effective implementation of obligations.[83]

A proposal was put forward for developing a legislative regime drawing on legislation in other countries and building on the Canadian Standards Association Model Code. According to the proposal, the Canadian legislation should:

- foster responsible privacy practices by those in the private sector who hold personal information;
- provide light but effective guidance for protecting enforceable rights and a level playing field in the marketplace, where personal information is an increasingly important element;
- be flexible, simple and effective, and consumer-friendly, with enforceable rights and effective means for redress;
- be cost-effective and administratively efficient and not overly burdensome for industry, especially small businesses; and
- conform to Canada's international obligations and trade agreements.[84]

(82) Canada, Task Force on Electronic Commerce, Industry Canada, Justice Canada, *The Protection of Personal Information: Building Canada's Information Economy and Society*, Ottawa, January 1998, p. 6.

(83) *Ibid*., p. 11.

(84) *Ibid*.

I. Canadian Standards Association -- Model Code for the Protection of Personal Information

As the federal government was formulating its policy on privacy protection, the Canadian Standards Association (CSA) had established a multi-stakeholder committee of representatives of business, government and consumer groups to develop a model code on the protection of personal information. This process produced the 1996 CSA *Model Code for the Protection of Personal Information*.(85) This sets out 10 principles on privacy and an individual's right of access to information. Founded on the OECD Guidelines, these principles include:

Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with certain principles.

Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Limiting Use, Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

Accuracy: Personal information shall be as accurate, complete and up-to-date as necessary for the purposes for which it is used.

Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of information.

Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An

(85) Canadian Standards Association, Model Code for the Protection of Personal Information: A National Standard of Canada, CAN/CSA-Q830-96, 1996.

individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

The CSA Model Code was designed to serve as a model that could be adopted by businesses and modified to suit their particular circumstances. It has been included as part of Bill C-6, the Personal Information Protection and Electronic Documents Act.

J. Uniform Law Conference of Canada

In 1996, the Uniform Law Conference of Canada (ULCC), an independent body that promotes the uniformity of legislation across Canada, recommended the development of a uniform data protection law that would regulate how personal information in the private sector would be protected. The ULCC began work on a draft Uniform Data Protection Act that would:

- apply equally to all businesses and non-government organizations, regardless of size or type of activity;
- treat all personal data in the same way, regardless of their differing sensitivity;
- be based on established data protection principles such as those found in the Canadian Standards Association Model Code for the Protection of Personal Information;
- establish an administrative mechanism to oversee the implementation of the law (such as existing data protection commissions);
- provide the data protection commission with the power to educate the public about data protection in the private sector;
- investigate and mediate complaints, but only after the company complaint process had been tried first (assuming there was a company complaint process and that the process had clear and short timelines) while allowing for exceptional cases where a complaint could go directly to the commission);
- allow the commission to publish the names of companies that did not comply with the data protection law; and

- include an offence provision for violation of the law.(86)

The ULCC's work on a uniform privacy law was suspended in 1998, however, after the introduction of federal legislation to protect privacy in the private sector.

FEDERAL LEGISLATION: BILL C-6 -- PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

On 1 October 1998, the federal Minister of Industry introduced Bill C-54, the Personal Information Protection and Electronic Documents Act, in the House of Commons. The bill was referred to the House of Commons Standing Committee on Industry for review and subsequently reported back to the House of Commons with several amendments. Bill C-54 died on the Order Paper with the prorogation of Parliament, however, and was reintroduced as Bill C-6 on 15 October 1999.(87) Bill C-6 is scheduled to come into effect in 2001.

Bill C-6 contains measures to protect personal information in the private sector, creates an electronic alternative for doing business with the federal government, and clarifies how the courts assess the reliability of electronic records used as evidence.

The bill is divided into six parts. Part 1, entitled "Protection of Personal Information in the Private Sector," along with Schedule 1, which contains the CSA Model Code, creates rules for the collection, use and disclosure of, as well as access to, personal information in the private sector. Part 2, entitled "Electronic Documents," provides for the use of electronic alternatives where federal laws now provide for the use of paper to record or communicate information. The other parts would amend other federal statutes to facilitate the use and legal recognition of electronic documents. Part I is described in some detail and Part 2 is briefly considered below.

---

(86) Uniform Law Conference of Canada, *Data Protection in the Private Sector: Options for a Uniform Statute*, 1996, p. 1.

(87) Bill C-6 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, 2nd Session, 36th Parliament, 48 Elizabeth II, 1999.

A. Part 1

Part 1 of Bill C-6 (sections 2 to 30) sets out definitions, the purpose of the Part, its scope of application, a "purposes limitation" requirement, and exemptions that would allow an organization to collect, use and disclose personal information without the knowledge or consent of the individual concerned. Part 1 also contains provisions pertaining to an individual's access to his or her personal information, and the Privacy Commissioner's powers of investigation and audit.

Section 2 of the bill contains a number of definitions, the most notable of which are "commercial activity," "organization" and "personal information." "Commercial activity" is defined as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists." "Organization" includes an association, a partnership, a person and a trade union." "Personal information" is defined 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."

The purpose of Part 1 is to establish rules to govern the collection, use and disclosure of personal information that would recognize both the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use and disclose information for purposes that a reasonable person would consider appropriate. The goal is to balance an individual's right to privacy against the reasonable needs of organizations to collect, use and disclose information for economic purposes.

1. Application of the Law

Subject to certain exceptions, Part 1 of the bill would apply to every organization that collects, uses or discloses personal information in the course of commercial activities. It would also apply to the collection, use and disclosure of personal information pertaining to the employees of federally regulated organizations.

Part 1 would not apply, however,

- to any government institution to which the federal *Privacy Act* applies;

- to personal information collected, used or disclosed by an individual exclusively for personal or domestic purposes; or

- to organizations in respect of personal information that is collected, used or disclosed for journalistic, artistic or literary purposes.(88)

The health sector, however, will have one year from the date that Part 1 comes into force to meet the requirements of the law. This does not exempt the health sector from the legislation but rather gives it additional time in which to prepare for implementing the law.

Section 30(1) sets out an important exclusion with respect to the application of the bill. It provides that Part 1 will not apply to "any organization in respect of personal information that it collects, uses or discloses within a province whose legislature has the power to regulate the collection, use or disclosure of the information, unless the organization does it in connection with the operation of a federal work, undertaking or business or the organization discloses the information outside the province for consideration." Section 30(2) states that the exclusion of the application of Part 1 within a province will cease to have effect three years after section 30 comes into force.

Thus, after Part I comes into force, it will apply to the federally regulated private sector (telecommunications, broadcasting, banking, interprovincial transportation, and airline industries). Part 1 will also apply to organizations that collect, use or disclose personal information within a province if the organizations disclose that information interprovincially or internationally for commercial purposes. Three years after Part 1 comes into force, however, it will apply more broadly, to organizations that are located entirely within a province, even if they collect, use or disclose personal information only within that province.

A province can enact its own legislation to protect the privacy of personal information that is collected, used or disclosed within its boundaries. Under section 26(2)(b), the Governor in Council can exempt an organization, class of organizations, activity or class of activities from the application of Part 1, if a province has adopted legislation that is "substantially similar" to Part 1. This exemption is limited, however, to the collection, use or disclosure of personal information that takes place within a province. Interprovincial or international trade in personal information will still be subject to Bill C-6. At the present time,

(88) *Ibid*., subsection 4(1).

Quebec is the only province that has enacted legislation governing the collection, use and disclosure of personal information in the private sector.

Section 5 requires organizations to comply with the obligations set out in the CSA Model Code (included in the bill as Schedule 1) unless the exceptions contained in sections 6 to 9 apply. But it also provides that the use of the word "should" in Schedule 1 indicates a recommendation and does not impose an obligation. Section 5 goes on to set out a "purposes" test by stating that the purposes for which an organization can collect, use or disclose personal information are to be limited to those that "a reasonable person would consider are appropriate in the circumstances."

2. Exemptions

Section 7, which sets out the exemptions under which an organization can collect, use or disclose personal information without the knowledge or consent of the individual concerned, is critical to the operation of the bill's privacy regime.

Section 7(1) provides that an organization can collect personal information without an individual's knowledge or consent only where:

> (a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
>
> (b) it is reasonable to expect that obtaining the individual's consent to collection will compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;
>
> (c) the collection is solely for journalistic, artistic or literary purposes; or
>
> (d) the information is publicly available and is specified by regulations under the bill.

Section 7(2) provides an exemption to the knowledge or consent requirement with respect to the use of personal information where:

> (a) an organization becomes aware of information that it has reasonable grounds to believe can be useful in the investigation of a

> contravention of the laws of Canada, a province or a foreign jurisdiction;
>
> (b) the information is used to act in an emergency that threatens the life, health or security of an individual;
>
> (c) subject to certain conditions, the information is used for statistical, or scholarly study or research purposes;
>
> (c.1) the information is publicly available and is specified by regulations under the bill; or
>
> (d) the information was collected under section 7(1)(a) or (b).

Under section 7(3), an organization can disclose personal information without an individual's knowledge or consent if the disclosure is:

> (a) made to legal counsel representing the organization;
>
> (b) for the purpose of collecting a debt owed by the individual to the organization;
>
> (c) required to comply with a subpoena or warrant issued or an order made to compel the production of information, or to comply with the rules of the court relating to the production of records;
>
> (c.1) to a government institution for the purposes of national security, defence, conducting international affairs, law enforcement or investigation or administering federal or provincial law;
>
> (d) made to an investigative body where the organization reasonably believes that the information relates to a breach of an agreement or a contravention of a law, or suspects that the information relates to national security, defence, or the conduct of international affairs;
>
> (e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual;
>
> (f) subject to certain conditions, for statistical or scholarly study or research purposes;
>
> (g) made to historical or archival institutions;

> (h) made after the earlier of 100 years after the creation of the record containing the information, or 20 years after the death of the individual about whom the information relates;
>
> (h.1) of publicly available information as specified by the regulations;
> (h.2) made by an investigative body and disclosure is related to investigating a breach of an agreement or a contravention of a law;
>
> (i) required by law.

As noted above, the exemption for the use of personal information for "statistical, or scholarly study or research purposes" is subject to certain conditions. It can be invoked only if the purposes cannot be achieved without using the information, the confidentiality of the information is ensured, it is impracticable to obtain consent; and the organization informs the Privacy Commissioner of the use. Similarly, the exemption for disclosure for statistical, or scholarly study or research purposes is allowed if all of these conditions except an assurance of confidentiality are met.

3. Access to Personal Information

Bill C-6 provides individuals with a right to have access to their personal information and to have it corrected, if necessary. An organization must respond to a request for access within 30 days, but can extend this time limit under certain conditions.[89] It can refuse to give an individual access to his or her personal information where this would reveal personal information about a third party and the third-party information cannot be severed from the record. If the third party consents, however, or if the individual needs the information because his or her life, health or security is threatened, the third-party prohibition will not apply.

Furthermore, an organization can refuse to give access to personal information where:

- the information is protected by solicitor-client privilege;
- access would reveal confidential commercial information;
- access can reasonably be expected to threaten the life or security of another individual;

(89) *Ibid*., section 8.

- the information was collected for purposes related to breach of an agreement or the detection of an offence under federal or provincial law; or

- the information was generated in the course of a formal dispute resolution process.(90)

Access is permitted, however, if the individual needs the information because his or her life, health or security is threatened.

The bill gives individuals the right to complain to the federal Privacy Commissioner about an organization's compliance with the legislation or the CSA Code and authorizes the Commissioner to investigate and try to resolve the complaint.

Section 11 provides that a complaint can be initiated either by an individual or by the Commissioner. An individual can file a complaint against an organization for contravening provisions of the bill relating to collection, use, disclosure of or access to personal information or for not following a recommendation set out in the Model Code. The Commissioner, however, can initiate a complaint only if satisfied that there are reasonable grounds to investigate a matter under Part 1 of the bill.

4. Powers of the Privacy Commissioner

The bill confers broad powers on the Privacy Commissioner. These include the authority to:

- receive complaints from individuals and initiate complaints;

- conduct investigations in relation to complaints;

- attempt to resolve complaints through mediation and conciliation;

- within one year after the filing or initiation of a complaint, prepare a report in relation to the complaint;

- in respect of a complaint that the Commissioner does not initiate: with the consent of the complainant, apply to the Federal Court-Trial Division for a hearing; appear before the Court on behalf of a complainant who has applied for a hearing; or, with leave of the Court, appear as a party to a hearing;

---

(90) *Ibid*., section 9.

- audit the personal information management practices of an organization where the Commissioner has reasonable grounds to believe that the organization is contravening the provisions of the legislation pertaining to the protection of personal information or is not following a recommendation set out in the CSA Model Code;

- make public any information relating to an organization's personal information management practices where the Commissioner believes that it is in the public interest to do so;

- consult with his or her provincial counterparts who, under substantially similar legislation, have powers and duties similar to those of the Commissioner;

- enter into agreements with his or her provincial counterparts to coordinate activities, undertake and publish research and develop model contracts for the protection of personal information that is collected, used or disclosed interprovincially or internationally;

- develop and conduct information programs to foster public understanding of the purposes of the privacy protection provisions, undertake and publish research related to the protection of personal information and encourage organizations to develop detailed policies and practices as well as codes of practice;

- report annually to Parliament.

Section 12 gives the Commissioner broad powers for the purpose of investigating complaints. These include the power to:

- summon and enforce the appearance of persons and to compel them to give evidence and produce records;

- administer oaths;

- receive evidence whether or not it is admissible in a court of law;

- enter the premises of an organization at any reasonable time;

- converse in private with any person in the premises; and

- examine and obtain copies or extracts from records found in the premises.

The bill also provides for a court hearing before the Federal Court-Trial Division. A complainant can request a hearing within 45 days after receiving the Commissioner's report. Among other things, the Court has the power to order an organization to correct its practices if

they do not comply with the law; publish notices of any action taken to correct its practices; and order remedies including damages for humiliation suffered by a complainant.(91)

The bill creates offences for obstructing the Commissioner in an investigation, destroying records before all recourse is exhausted, or dismissing, suspending, or demoting an employee who discloses a violation of the Act by his or her employer. The bill provides for a maximum fine of $100,000.(92)

Under section 27.1, employees who disclose a contravention of the Act on the part of their employers or others are protected against dismissal, suspension, demotion, discipline or harassment.

B. Part 2

Part 2 of Bill C-6 provides for the use of electronic alternatives to paper in communicating with the federal government and introduces the concept of a "secure electronic signature" in such transactions. Pursuant to the legislation, the government will prescribe technologies or processes for defining "secure electronic signature" based on the following criteria:(93)

- the electronic signature must be unique to the person using it;
- the person whose electronic signature is on the document must have control of the use of the technology to attach the signature;
- the technology can be used to identify the person using the electronic signature; and
- the electronic signature can be linked to an electronic document to determine if the document has been changed after the electronic signature was attached to it.

The bill also deals with electronic documents used as evidence in legal proceedings. In a typical court proceeding, original documents are usually required to satisfy a

(91) *Ibid*., section 16.

(92) *Ibid*., section 28.

(93) For the purposes of Bill C-6, "electronic signature" means a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document; a "secure electronic signature" is an electronic signature that results from the application of a technology or process prescribed by regulations under section 48(1) of the bill.

court that the terms and conditions of an agreement have not been changed since it was signed. This requirement is difficult to satisfy where electronic documents are involved because the original cannot be distinguished from an amended document and because the document is not authenticated by hand-written signatures. The bill, therefore, requires the use of secure electronic signatures for electronic documents whenever the law provides for original documents or statements of truth.

DEVELOPMENTS AT THE PROVINCIAL LEVEL

A. Quebec

The first jurisdiction in North America to enact legislation pertaining to the collection, use, disclosure and retention of personal information in the private sector was Quebec.(94) To date, it is still the only province with such legislation. The Quebec *Act respecting the protection of personal information in the private sector* (Bill 68) came into force on 1 January 1994.(95)

The Act deals with the collection of "personal information," which it defines as information about an individual and from which the individual can be identified. Except as otherwise provided in the Act, the consent of the individual concerned is required for the collection, use and transfer of his or her personal information. The Quebec statute requires that consent must be manifest, free and enlightened and must be given for specific purposes. In addition, consent is valid only for the length of time needed to achieve the purposes for which it was requested. A business may collect information from a third person without the consent of the person concerned, if the law otherwise permits or if other conditions set out in the Act are present. At the time it collects the information, a business is required to inform the individual of the use that will be made of it.

The Act also sets out rules respecting the holding of personal information, whereby individuals may have deleted from their files any information that is obsolete or not

(94) This section relies heavily on the description of the Quebec privacy legislation found in Richard C. Owens, *Privacy and Financial Services in Canada*, Research Paper Prepared for the Task Force on the Future of the Canadian Financial Services Sector, September 1998, p. 65-68.

(95) R. S.Q. c. P. 39.1.

justified for the purposes of the files. Personal information must be current and accurate when it is used to make a decision affecting an individual. A business must inform individuals of the existence and object of files that are held about them as well as their right to have access to these.

Generally, businesses are proscribed from disclosing, transferring or using personal information for purposes that are "not relevant" to the object of the individual's file. Other uses, disclosures or transfers are permitted where the individual's consent has been obtained or where an exception in the Act applies. The Act also prohibits Quebec businesses from transferring personal information to parties outside the province unless the transferor has taken "all reasonable steps to ensure that the information will not be used for purposes not relevant to the object of the file."

Special provisions apply to "nominative lists," -- lists of individuals' names, addresses, and phone numbers. When a business wants to use its own nominative list for commercial or philanthropic canvassing, the individuals named on the list must be given the opportunity to have their names removed from the list.

The Act also provides for access to and correction of personal information at the individual's request. A business must confirm the existence of a file containing personal information and respond to an access request within 30 days. However, there are exemptions and limits to the access provisions.

The Act provides for recourse to the Quebec Commission d'accès à l'information where there is a disagreement between an individual and a business about the application of the law. Commission decisions are binding on the parties, though they may be appealed.

A business that collects, holds or communicates information in a manner contrary to the statute is liable to fines of $1,000 to $10,000 for a first offence and $10,000 to $20,000 for a second or later offence. Directors or administrators of businesses may be found personally liable where they authorized, ordered or consented to the offending act.

The Quebec law does not provide for privacy codes for various business sectors.

B. New Brunswick

In May 1998, the New Brunswick Department of Justice released a discussion paper in which it examined the extension of privacy legislation to the private sector.(96) The purpose of the paper was to establish whether there was a need for a greater level of privacy protection than the law currently provides and, if so, by what means it should be provided. The Paper consists of "Propositions" for discussion and is to be referred to the Law Amendments Committee of the New Brunswick legislature for review and public discussion.

Suggesting that the Canadian Standards Association Model Code for the Protection of Personal Information should be the starting point for privacy protection legislation, the Paper points out that the scope and content of legislation based on the CSA Code would likely be broad and that the key elements of the CSA Code for legislative purposes would be the Code's ten principles.

The Discussion Paper examines whether the CSA Principles should apply equally to small and large organizations. It asks whether private sector data protection legislation should be as broad as the CSA Code aims to be, or whether a more focused approach would be more appropriate. The Paper notes that data protection legislation must be careful not to impose on small organizations levels of obligation that they cannot reasonably be expected to achieve.

The Paper also looks at the enforcement of possible data protection legislation based on the CSA Code. It discusses whether penal remedies, civil remedies or administrative remedies might be appropriate.

C. Manitoba

In 1997, the Manitoba Information Highway Advisory Council stated that it was in Manitoba's interest to take a leadership role in striking a "balance between protecting the privacy of personal and confidential information and ensuring access to information for legitimate social and economic purposes."(97) Among other things, it recommended that the Manitoba government should "strongly encourage the private sector to consider adopting

(96) New Brunswick, Department of Justice, *Privacy Discussion Paper #2,* May 1998.

(97) *The Report of the Manitoba Information Highway Advisory Council,* 1997, p. 44.

guidelines, such as those published by the Canadian Standards Association, regarding information access and privacy protection."[98]

In 1997, Manitoba enacted the *Personal Health Information Act*, which regulates the collection, use and disclosure of personal health information. The Act applies to personal health information that is recorded about individuals who can be identified, but not to statistical information or data used in such a way as to maintain the confidentiality of individuals.[99]

The Act gives individuals the right to see their personal health information, copy it and request a correction. The Act protects the privacy and confidentiality of information through a number of provisions, such as:

- limiting the nature and amount of information that can be collected, used or disclosed;
- requiring that individuals must be informed about why the information is being collected;
- having information updated and corrected before it can be used or disclosed;
- requiring implementation of and compliance with policies governing maintenance and destruction of the information;
- requiring the adoption of reasonable administrative, technical and physical safeguards to ensure the confidentiality, security, accuracy and integrity of the information;
- prohibiting the sale of personal health information; and
- requiring that the use of government-held personal health information for research must be approved by a health information privacy committee.

Offences under the Act include:

- collecting, using, selling or disclosing personal health information in violation of the Act;
- failing to retain personal health information in a secure manner; and

(98) *Ibid*., p. 49.

(99) Much of the information about the contents of the *Personal Health Information Act* comes from the press release of the Manitoba Minister of Health, "Personal Health Information Act Proclaimed," 17 December 1997, http://www.gov.mb.ca/chc/press/top/1997/12/1997-12-17-02.html

- deliberately erasing or destroying personal health information to prevent someone from having access to it.

The provincial Ombudsman has responsibility for overseeing compliance with the Act and handling complaints from individuals with respect to their rights of access and the collection, use and disclosure of personal health information.

In March 1999, the Manitoba Minister of Consumer and Corporate Affairs released the discussion paper *The Protection of Personal Information in the Private Sector*, in order to elicit the views of Manitobans on privacy protection. The Paper sets out 12 specific questions on which the government was seeking public input. Among other things, the Paper describes the vital role that information plays in the economy and the operation of government, the growing concern about how personal information is gathered, privacy protection approaches and initiatives in the United States, the European Union and Canada through the CSA Model Code, Bill C-54 (now Bill C-6) and developments in Manitoba, including the report of the Manitoba Information Highway Advisory Council. The Paper observes that protecting the privacy of personal information is not a simple issue and suggests that Manitoba must carefully consider the impact of federal privacy legislation on Manitoba consumers and private-sector organizations.(100)

D. British Columbia

In July 1999, the British Columbia government appointed an all-party Special Committee to review and make recommendations on the protection of personal information in private sector transactions and the impact of electronic documents on privacy and freedom of information for residents of British Columbia. Following upon this, in October 1999, the British Columbia Information, Science and Technology Agency released a discussion paper, *Protecting Personal Privacy in the Private Sector*.(101)

The Discussion Paper observes that "British Columbians should have an effective regulatory framework to protect personal information, and be informed as to their rights." It

(100) Manitoba, Department of Consumer and Corporate Affairs, *The Protection of Personal Information in the Private Sector*, March 1999, http://www.gov.mb.ca/cca/papereng.pdf

goes on to suggest that "an effective response will depend on a blend of solutions, including consumer education, privacy-enhancing technologies, codes of practice and standards, and/or legislation with some form of oversight provision."(102) The Paper states that there is a need to protect individuals from improper collection, use and disclosure of their personal information especially in areas that will not be covered by Bill C-6.(103)

The Paper poses 10 questions as a catalyst for discussion.

SELF-REGULATION

A number of businesses, industry groups and private sector organizations have sought to implement fair information practices by developing and adopting voluntary guidelines and codes of practice. Some of the better known codes are those of the Canadian Bankers Association, the Canadian Marketing Association, the Canadian Life and Health Insurance Association and the Insurance Bureau of Canada. Generally, such codes can be broken down into five different categories.

Individual Company Codes: codes that have been developed by companies in the absence of, or in anticipation of wider sectoral instruments.

Sectoral Codes of Practice: codes that have been developed by an industry group recognizing the need for consistency of policy and practice while establishing a set of rules tailored to the needs of the industry and pre-existing regulatory framework for the sector.

Functional Codes: codes that have been defined by the practice in which an organization is engaged.

Technological Codes: codes that address specific invasive practices involving information and communication technology.

(cont'd)

(101) British Columbia, Information, Science and Technology Agency, *Protecting Personal Privacy in the Private Sector*, October 1999, http://www.ista.gov.bc.ca/FOI_POP/PSP_100799.htm

(102) *Ibid*., p. 7.

(103) *Ibid*. The Paper notes that the federal legislation will not protect the records of employees of provincially regulated private sector businesses or personal information collected in non-commercial activities such as private hospitals, private schools and charities.

Professional Codes: codes that have been developed for use by professional associations and societies.(104)

Voluntary codes of practice have been an important component of privacy protection initiatives in North America where legislation to protect the privacy of personal information in the private sector has been less developed. Indeed, the self-regulatory approach has been promoted by the U.S. federal administration as the system that will foster growth of electronic commerce.

A. Advantages and Disadvantages of Self-Regulation

There are both advantages and disadvantages to self-regulation. A number of these were discussed in the 1996 paper *Privacy Protection Models for the Private Sector* and are outlined below.

One of the most important advantages of self-regulation is flexibility. Advocates of self-regulation argue that a regulatory approach is too rigid, tends to lag behind advances in technology and uses of personal information, and is difficult to change. Self-regulation, on the other hand, allows businesses to quickly develop and implement policies and codes of conduct in response to new developments and issues, and to tailor codes of practice to the needs of a particular sector.(105) Voluntary codes also allow businesses to balance privacy with other possibly competing interests and the everyday practicalities of data processing and use.(106)

Consumers can benefit from a voluntary approach. Because voluntary codes tend to be specific to particular industries or issues, they are often more detailed and relevant than government legislation, which by its very nature must be broader in scope. Moreover, since codes tend to be administered closer to the level where disputes actually arise, a voluntary code may offer consumers more ready access to redress mechanisms.(107)

Another benefit of self-regulation is the absence of bureaucracy and government intervention. Proponents of self-regulation argue that regulation is costly and burdensome for

---

(104) Ann Cavoukian, *Privacy as a Fundamental Human Right vs. Economic Right: An Attempt at Reconciliation*, Information and Privacy Commissioner/Ontario, September 1999, p. 6.

(105) Tom Wright, *Privacy Protection Models for the Private Sector*, December 1996, p. 10.

(106) *Ibid*.

(107) *Ibid*.

industry, consumers and taxpayers alike. A self-regulatory approach avoids the creation of bureaucratic structures and the expenditure of government funds.(108)

Voluntary codes, however, have limitations. These include:

- a lack of meaningful enforcement measures and/or appeal mechanisms to independent third parties;
- ineffective or non-existent sanctions for non-compliance;
- inadequate remedies for breaches of a code;
- lack of independence of self-regulatory agencies;
- limited participation by private sector organizations; and
- failure to incorporate objectively fair standards for data protection.(109)

Research has pointed out weaknesses in the privacy codes adopted by Canadian organizations. A study of 12 voluntary codes adopted by Canadian organizations, conducted by the Public Interest Advocacy Centre and referred to in the paper *Privacy Protection Models for the Private Sector*, found weaknesses in a number of codes of practice and concluded that the codes did not adequately protect privacy. Among the problems found were:

- low consumer involvement in code development;
- consumer exclusion from code administration;
- administration at either the firm or industry level;
- low use of publicity as a compliance tool;
- inadequate code coverage;
- inadequate monitoring;
- low levels of compliance;
- weak sanctions; and
- no ultimate means of consumer recourse.(110)

(108) *Ibid*.

(109) *Ibid*., p. 10-11.

(110) *Ibid*., p. 11.

B. Measures to Improve Private Sector Privacy Codes and Policies

Developing a privacy policy or code of practice and posting it on a Web site is often not enough to provide adequate protection for personal information. To improve the level of privacy protection and to provide online consumers with a measure of certainty that the privacy of their personal information will be protected, voluntary programs have been developed by non-governmental organizations in which Web sites can participate and in this way assure users that their privacy policies comply with certain privacy principles.

Three of the most recognizable voluntary programs are TRUSTe, CAWebTrust and BBBOnline.

1. TRUSTe

Web sites that comply with TRUSTe's established privacy principles and agree to comply with its oversight and consumer dispute resolution process can display the TRUSTe logo or seal. The displayed mark signifies to users that the Web site will state "what personal information is being gathered, how it will be used, with whom it will be shared, who is gathering the information, what options the user has, what security procedures are in place to prevent misuse or loss and how users can correct information to control its dissemination."(111)

Businesses that are part of the TRUSTe program undergo periodic assessments to ensure that they are in compliance with privacy principles.

2. CAWebTrust

CAWebTrust is a program jointly developed by the American Institute of Public Accountants and the Canadian Institute of Chartered Accountants. A Web site that has met the WebTrust principles can display the WebTrust seal and thereby ensure consumers that the site meets WebTrust principles and criteria relating to the disclosure of business practices, transaction integrity and information protection.

To maintain the WebTrust certification, a site must be evaluated at least every three months.(112)

---

(111) TRUSTe, Frequently Asked Questions, http://www.truste.org/webpublishers/pub_faqs.html

(112) WebTrust, http://www.cica.ca/cica/cicawebsite.nsf/public/SPWTe_generalfaqs

3. BBBOnline

In the United States, the Council of Better Business Bureaus (CBBB) has developed a self-regulatory online privacy program through a subsidiary BBBOnLine.

Like TRUSTe and CAWebTrust, the BBBOnline program allows organizations to display the BBBOnline seal on their Web sites after demonstrating that they have adopted and implemented privacy policies that meet BBBOnLine Privacy Program requirements.

Among other things, BBBOnline program participants must agree to:[113]

- cooperate in applicable program verification requirements;
- participate in the BBBOnLine Privacy Policy Dispute Resolution Program and abide by decisions made under that program;
- inform BBBOnLine of all material changes to their privacy policies or practices;
- take reasonable steps to ensure that individually identifiable information collected online is secure from unauthorized access;
- allow individuals the opportunity to opt-out or otherwise prohibit unrelated uses of individually identifiable information about them;
- provide individuals with a choice regarding the transfer of information to third parties for marketing purposes;
- assure that information collected online is accurate, complete and timely for the purpose(s) for which it is to be used and provide individuals with access to individually identifiable information collected from them online;
- have a privacy policy that is easy to read and disclose in clear and simple language:
    1. who is collecting the information,
    2. the type(s) and intended use(s) of the individually identifiable information being collected,
    3. the choices individuals have about the way such information is used and to whom it is disclosed,
    4. the collector’s commitment to data security,
    5. an appropriate contact method regarding the website’s privacy policy,
    6. the seal participant’s participation in the BBBOnLine Privacy Program and information on how individuals may learn more about that program,

(113) BBBOnline, http://www.bbbonline.org/businesses/privacy/eligibility.html

7. any corporate subsidiaries, operating divisions or related product lines that are excluded from the privacy program,
8. any individually identifiable information collected at the site that is shared with contractors, corporate affiliates or other third party agents not covered by a common privacy policy,
9. the choices available to users with regard to information shared with affiliates or third party agents not covered by a common privacy policy,
10. the steps participants take to assure the accuracy of individually identifiable information that it maintains in identifiable form,
11. the process available to individuals to obtain access their personal information collected online and to correct errors in that information,
12. whether any other organization collects individually identifiable information at the site as the result of transacting business with the individual at the site,
13. any information collection that is not covered by the privacy policy.

Some 1,000 Web sites carry privacy seals from at least one of these third-party enforcement services.

4. Online Privacy Alliance

Another organization, the Online Privacy Alliance, was formed in the United States in 1998 to promote the self-regulation of consumer privacy online. Today, the Alliance has a membership of about 90 global companies and associations. Members of the Alliance commit themselves to implement online privacy policies consistent with the Alliance's guidelines and to participate in effective self-regulatory enforcement mechanisms.

Upon joining the Online Privacy Alliance, each member organization agrees that its policies for protecting individually identifiable information in an online or electronic commerce environment will address, at a minimum, the following elements:

- *adoption and implementation of a privacy policy*: a business engaged in electronic commerce should establish a policy for protecting the privacy of individually identifiable information;

- *notice and disclosure*: an organization's privacy policy must be easy to find, read and understand, available prior to or at the time that individually identifiable information is collected or requested, state clearly what information is being collected and the use of that information; indicate possible third-party distribution of the information; state the choices available to an individual regarding collection, use and distribution of the collected information; contain a statement of the organization's commitment to data security and what steps the organization takes to

ensure data quality and access; and provide a clear statement of what accountability mechanism the organization uses, including how to contact the organization;

- *choice/consent*: individuals must be given the opportunity to decide how individually identifiable information collected from them online may be used when the use is unrelated to the purpose for which the information was collected;

- *data security*: the reliability of individually identifiable information should be assured and the information protected from loss, misuse or alteration;

- *data quality and access*: organizations creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to assure that the data are accurate, complete and timely for the purposes for which they are to be used and establish mechanisms to correct inaccuracies in the information.(114)

The U.S. Administration credits organizations such as the Online Privacy Alliance, TRUSTe, BBBOnline, and CA WebTrust with much of the progress in the development of private sector privacy codes in the U.S.(115)

CONCLUSIONS

Over the last two decades, protecting the privacy of personal information has become an important public policy issue. The initial concerns about the collection and use of such information were with respect to the vast amounts of data held by governments. As a result, many jurisdictions moved to enact privacy legislation to govern the collection and use of information by the public sector. Since then, the focus has turned to the collection and use of personal information by the private sector. Businesses collect large amounts of information generated from a diverse array of sources, including consumer purchases, information voluntarily given by consumers and technology that tracks activity on the Internet.

Rapid advances in technology have increased the ability of businesses to collect, use and disseminate information about individuals in ways that were not possible only a few years ago. These advances have spawned fear that personal information will be used in ways that a person might not anticipate or without a person's knowledge or consent.

---

(114) Online Privacy Alliance, http://www.privacyalliance.org/

(115) *Towards Digital eQuality*, 1999, p. 36.

With the growth and development of electronic commerce has come a concomitant increase in the level of concern about maintaining privacy when doing business online. Surveys indicate that the protection of personal privacy is a key concern of many people in relation to electronic commerce and until such concerns are satisfactorily addressed the full potential of online commerce will likely remain untapped.

Privacy concerns are not, however, the only factor fuelling the demand for increased levels of privacy protection in the private sector. International trade patterns are also prompting the introduction of privacy protection measures. Now more than ever, businesses are operating in a global environment. Businesses that collect, retain, use or disclose personal information must be increasingly cognizant that privacy protection has become important to international trade. The European Union Directive on Data Protection, for example, restricts the transfer of personal information from EU member countries to other countries that do not have adequate levels of privacy protection.

Businesses have also come to recognize that privacy protection is good for them. Indeed, countries and business that can ensure consumers that that they have adopted measures to protect the privacy of personal information may have a competitive advantage over those who do not.

While it is generally acknowledged that measures must be adopted to protect the privacy of personal information, particularly in an online environment, and that such measures will be important to the future of electronic commerce, there has been considerable debate about whether government regulation or industry self-regulation is the best approach to providing such protection.

Thus far, a variety of privacy protection models have been developed. The EU Directive on Data Protection requires the adoption of a legislative model. In implementing the Directive, the U.K. *Data Protection Act 1998,* sets out a detailed legislative scheme for protecting personal information in the private sector. While the Act contemplates the use privacy codes adopted by trade associations or other bodies, such codes do not have statutory recognition. Even so, they are likely to play an important role in the interpretation and the enforcement of the Act.

In Canada, federal legislation to protect the privacy of personal information in the private sector has been passed and is scheduled to come into force in 2001. Like the U.K data

protection law, the Canadian *Personal Information Protection and Electronic Documents Act* contemplates the use of private sector privacy codes but does confer any kind of legal status on them.

Proposed privacy legislation in Australia, however, would go a step further by giving the force of law to codes that had been approved by the Privacy Commissioner. Upon approval, a code would replace the privacy principles to be set out in the legislation.

The United States has consistently refused to introduce private sector privacy legislation except in the area of children's online privacy. Strongly supporting industry self-regulation, the U.S. Administration has encouraged the development of industry codes of practice and privacy protection. To date, self-regulatory measures have received mixed reviews. One study found that the privacy protection policies of several Web sites did not reflect the necessary elements of Fair Information Practices and were unlikely to provide meaningful privacy protection. Other studies report better results. The creation of third-party privacy monitoring and dispute resolution services, however, is seen as important to the development of adequate self-regulatory privacy protection initiatives.

The adoption of an industry self-regulatory approach by the U.S. has been a trade irritant between the U.S. and the European Union and is the subject of ongoing negotiations for reaching an agreement as to whether self-regulation will meet the EU's "adequacy" standard for the transfer of personal data from EU to non-EU countries.

It is too early to state definitively whether the regulatory approach will win out over self-regulation. The most likely scenario is some combination of the two. Even where legislation exists and privacy codes have no legal status, it will be important for various industries to develop codes to reflect and put into operation the basic principles set out in the legislation and tailor the legislation to the circumstances of their particular industries. Where privacy codes are to be the mainstay of privacy protection, however, legislation may have to be developed to establish a baseline level; this would appear to be the approach adopted in Australia. The U.S. self-regulatory approach will likely work if the vast majority of enterprises doing business over the Internet adopt privacy protection measures that adhere to the principles of fair information practices and demonstrate through membership in third-party monitoring and dispute resolution services that they are providing an adequate level of privacy protection. If too few businesses participate or privacy protection measures prove inadequate, it may be necessary for the U.S. to change its position and consider legislative measures.