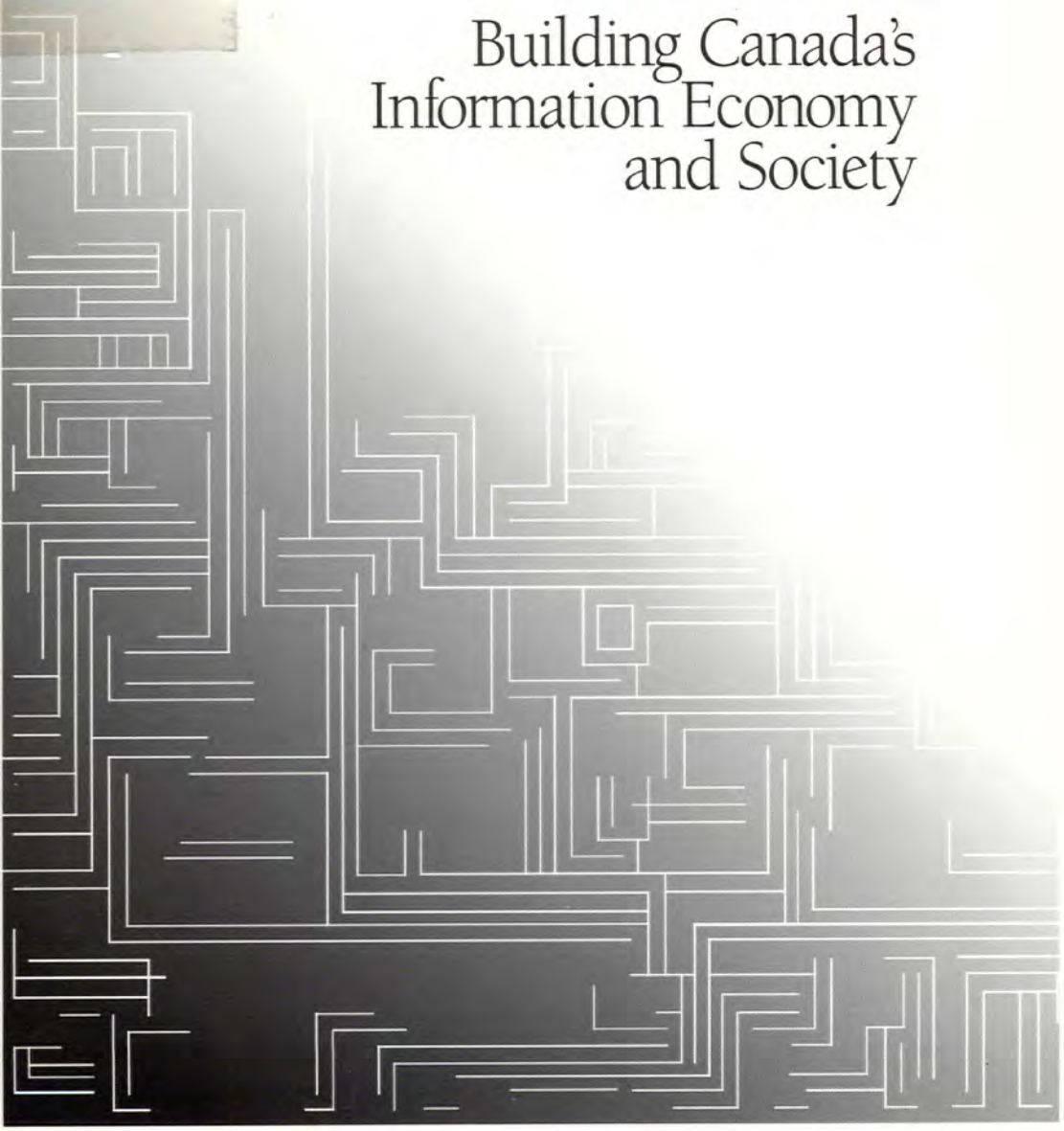
Government of Canada / Gouvernement du Canada

The Protection of Personal Information

Building Canada's Information Economy and Society



Canada

The Protection of Personal Information

Building Canada's Information Economy and Society

Task Force on Electronic Commerce
Industry Canada
Justice Canada
January 1998

The Protection of Personal Information — Building Canada's Information Economy and Society is available electronically in both official languages, on the Industry Canada *Strategis* web site at: *http://strategis.ic.gc.ca/privacy*
It is also available on the Justice Canada web site at: *http://canada.justice.gc.ca*

This document can be made available in alternative formats for persons with disabilities upon request.

Additional print copies of this discussion paper are available from:

Distribution Services
Industry Canada
Room 205D, West Tower
235 Queen Street
Ottawa ON K1A 0H5
Tel.: (613) 947-7466
Fax: (613) 954-6436

For information about the contents of this discussion paper and the consultation process, or to submit your responses to the paper, please contact:

Helen McDonald
Director General, Policy Development
Task Force on Electronic Commerce
Industry Canada
20th Floor, 300 Slater Street
Ottawa ON K1A 0C8
Fax: (613) 957-8837
E-mail: privacy@ic.gc.ca

Telephone Enquiries: (613) 990-4255

Submissions must be received on or before March 27, 1998 and must cite the *Canada Gazette*, Part 1, Jan. 24, 1998, Notice Number IPPB-002-98 — Release of Public Discussion Paper on the Protection of Personal Information in the Marketplace and the title of this document.

Two weeks after the closing date for comments, all submissions will be made available for viewing by the public, during normal business hours at:

Industry Canada Library
3rd Floor West
235 Queen Street
Ottawa ON K1A 0H5

and at the regional offices of Industry Canada in Halifax, Montreal, Toronto, Edmonton and Vancouver for a period of one year.

Cat. No. C2-336/1998
ISBN 0-662-633-26-1
51730B

Contents

Introduction: Building Canada's Information Economy and Society

Connecting Canadians

"We will make the information and knowledge infrastructure accessible to all Canadians by the year 2000, thereby making Canada the most connected nation in the world . . . . A connected nation is more than wires, cables and computers. It is a nation in which citizens have access to the skills and knowledge they need to benefit from Canada's rapidly changing knowledge and information infrastructure. It is also a nation whose people are connected to each other."

Speech from the Throne, September 23, 1997.

Canada's success in the 21st century depends increasingly on the ability of all Canadians to participate and succeed in the global, knowledge-based economy. And to ensure that success, all of us together — individual citizens, the private sector and governments at all levels — must move quickly to build Canada's information economy and society. For its part, the Government of Canada is committed to helping Canadians access the information and knowledge that will enable them, their communities, their businesses and their institutions, to find new opportunities for learning, interacting, transacting and developing their economic and social potential.

That is what connecting Canadians is all about — discovering a world of economic and social opportunities by taking advantage of new technologies, information infrastructure, and multimedia content to spur business growth and development, create new and innovative jobs, improve our capacity to communicate directly with our fellow citizens and our public institutions and services, and extend our reach to other countries.

Electronic commerce, which is at the heart of the information economy, is the conduct of commercial activities and transactions by means of computer-based information and communications technologies. It generally involves the processing and transmission of digitized information. Examples of electronic commerce range from the exchange of vast amounts of financial assets between financial institutions, to electronic data interchange between wholesalers and retailers, to telephone banking, and to the purchase of products and services on the Internet.

For electronic commerce to flourish in Canada, it requires a clear, predictable and supportive environment where

citizens, institutions and businesses can feel comfortable, secure and confident. It also requires an international set of rules where citizens, institutions and businesses can easily exchange information, products and services across borders and around the world with predictable results and protection. This paper is one of a series related to electronic commerce which seeks your views on how to establish those clear and predictable rules that will make electronic commerce grow and thrive in Canada and will build Canada's information economy and society.

Protecting Personal Information

For Canada to become the most connected country in the world by the turn of the century, all of us — consumers, business and government — need to feel confident about how our personal information is gathered, stored, and used.

The challenge of the electronic age is that with each transaction we leave a data trail that can be compiled to provide a detailed record of our personal history and preferences. The digitization of health, education, employment and consumer records makes it possible to combine information and create an individual profile with data that most of us consider to be extremely personal. This information may be sent across provincial and national borders where it can be sold, reused or integrated with other databases without our knowledge or consent.

As consumers and citizens, we need to know that when we shop or plan a vacation on the Internet, bank from home, look for work, correspond with friends and family, make purchases without cash using debit cards, find medical information or engage in other forms of electronic transactions, we have some control over our information and can be assured that it enjoys a basic level of protection.

The Government of Canada is committed to setting clear and predictable rules governing the protection of personal information.

In May 1996, responding to a recommendation by the Information Highway Advisory Council, the Minister of Industry announced that the federal government would develop legislation to protect personal information in the private sector. In September 1996, the Minister of Justice reiterated this commitment and stipulated the government's intent to legislate by the year 2000. The Ministers of Industry and Justice have been jointly charged with developing the legislation, in consultation with the provinces and territories and with other stakeholders.

Legislation that strikes the right balance between the business need to gather, store, and use personal information and the consumer need to be informed about how that

information will be used and assured that the information will be protected is key to building the consumer trust and market certainty needed to make Canada a world leader in electronic commerce. At the same time, such legislation will provide our trading partners from around the world with the reassurance they need to engage in transactions that require cross-border transfers of personal information.

This discussion paper seeks your views on how to strike the right balance in the new legislation. It sets out the main issues that need to be addressed and outlines some options for the legislation, followed by some specific questions for your consideration. Your input is important; it will help ensure that the new legislation reflects a variety of interests while building the confidence of Canadians in electronic transactions.

Part 1: What is Privacy?

In repeated surveys, Canadians have expressed concern about privacy in general and about the loss of control over their personal information in particular. This kind of privacy is known as information privacy, and is defined as the right of individuals to determine when, how and to what extent they will share personal information about themselves with others.

Information privacy is important for a number of reasons. First, it is related to a series of other rights and values such as liberty, freedom of expression and freedom of association. Without some control over our personal information, our ability to enjoy these rights may be hindered.

Second, as more information about us becomes available, it is used in a wider variety of situations to make decisions about issues such as the kinds of services we are entitled to, the jobs we are qualified for and the benefits we may be eligible for. It is extremely important to have mechanisms in place to give us control over our own personal information and enable us to ensure that it is both accurate and relevant.

What Protection Exists Now?

The federal government and most provinces have legislation governing the public sector's collection, use and disclosure of personal information. The federal *Privacy Act* (1985) applies to all federal government departments, most federal agencies, and some federal Crown corporations. The Privacy Commissioner of Canada oversees the Act, and has powers to receive complaints, conduct investigations, and attempt to resolve disputes, among others. The Commissioner can also issue recommendations. Disputes about the right of access to personal information that are not resolved in this way can be taken to the Federal Court of Canada for judicial review.

The private sector is another matter. To date, only Quebec has adopted comprehensive privacy legislation for the private sector. Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* provides a detailed framework for the collection, use and disclosure of personal information. It is overseen by the Commission on Access to Information, which is responsible for conducting investigations and settling disputes.

In the rest of Canada, protection in the private sector is sporadic and uneven. Many industries are not

subject to any rules regarding the collection, use and disclosure of personal information, but a few are covered by what has been described by the Privacy Commissioner of Canada as a "patchwork" of laws, regulations and codes. The patchwork is made up of various federal and provincial laws, resulting in protection that is incomplete and possibly inconsistent. Effective as the patchwork may be in particular sectors, it does not establish common principles for all sectors and it does not cover all sectors. This incompleteness makes for uncertainty for business and a lack of uniform protection for consumers. And while the patchwork is useful as far as it goes, it is not adequate in the face of new developments.

Why Current Protection is No Longer Enough

New technologies, increasing data collection in the private sector, changing market trends and the new global marketplace for electronic commerce are contributing to the increasingly important role of information in the global economy. In the new global economy, information is a valuable commodity that can bring jobs, prosperity, and higher levels of customer service. This, along with a number of other key factors, is creating mounting pressure to collect and use personal information more broadly than ever before.

In an environment where over half of Canadians agree that the information highway is reducing the level of privacy in Canada,[1] ensuring consumer confidence is key to securing growth in the Canadian information economy. 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 where the misuse of personal information cannot result in a competitive advantage.

One key factor leading to increased pressure on current protection is the advances in network browsers and sophisticated software that mean that information is no longer kept solely in central databases but can be distributed over all the networks of an organization. This makes conventional geographic borders less and less relevant. And whereas in older, paper-based records systems, segregation of information was the norm, new systems make it easy and affordable to combine information from many sources to create a profile or to make decisions.

Another factor is that the emphasis in legislation on information held by the public sector does not reflect the reality that the private sector is now a major collector and user of personal information. Historically, the concern has been that governments hold a great deal of information about citizens, and this has prompted legislative action to put limits on the uses to

1. Ekos Research Associates Inc., "Information Highway and the Canadian Communication Household, Draft Wave 1 Report," January 1998.

which the information can be put and to provide citizens with opportunities to see and request correction of records about themselves. As we move increasingly into the information economy and society, however, and information itself becomes a commodity, the private sector is becoming an increasingly significant collector and user of personal information in the marketplace, and in third-party delivery of government services. It is important that this trend be reflected in new legislation that will ensure there are common guidelines for the handling and treatment of this information.

At the same time, the blurring of previously distinct market areas is another factor creating new pressures on existing rules and laws. For example, both cable and telephone companies now offer Internet access as part of their product line, as do many unregulated small businesses. Since these sectors are subject to different laws, this kind of convergence may create confusion for consumers about which rules apply to which companies, and under what circumstances, and whom they should complain to if there is a problem.

Some organizations have reacted positively to the privacy challenge and have developed voluntary codes to guide their collection and use of personal information. For example, the Canadian Direct Marketing Association requires its members to abide by a Code of Ethics that includes rules about the collection and use of personal information. The problem, however, is that not all direct marketers belong to the association, and there is no mechanism for ensuring that they abide by the same rules. Not all businesses or industry associations have undertaken voluntary measures, and there may be a short-term incentive for some companies to ignore such measures and to use personal information inappropriately. This can undermine fair competition in the marketplace, creating an unlevel playing field. It can also erode consumer confidence in an entire industry and create further confusion about rights and rules.

The ability to provide effective protection for personal information may be crucial to Canada's ability to remain competitive internationally in the global information economy. For example, it may affect the exchange of data with European Union member states. In 1995, the European Union enacted a *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*. The Directive is designed to harmonize data protection practices within the European Union. One of its requirements is for member states to adopt laws to protect personal information in both the public and private sectors. These laws must also include a provision to block transfers of information to non-member states that do not provide an "adequate" level of protection.

This Directive has the potential to make the protection of personal information a major non-tariff trade barrier with Canada. Failure to provide adequate protection for personal information may put Canada at risk of having "data flows" from the European Union blocked. Without comprehensive data protection legislation, Canadian businesses may be forced to undertake individual contractual negotiations to show compliance with the European Union rules. This process will be fraught with uncertainty and could become lengthy and expensive. It could also result in a higher standard of protection for information coming from outside the country than for information generated within our borders.

These and other pressures are likely to grow in the coming years. The global challenge to compete in the electronic commerce marketplace means that we do not have time for a slow, evolutionary approach to building up the protection of personal information and consumer trust. And citizens are also rightly asking for adequate protection in the new digital economy. It is therefore important to act now to develop legislation that will anticipate and adequately address both current and future challenges.

Protecting Personal Information: The Rules of the Road

Most efforts at legislating privacy begin with "fair information practices," which are sets of privacy principles. Fair information practices are guidelines for the collection, use, disclosure, retention and disposal of personal information.

Sets of fair information practices vary, but they generally include the following principles:

- ensuring public awareness and transparency (openness) of information policies and practices
- establishing necessity and relevance of the information collected
- building in finality (establishing the uses of the information in advance and eventually destroying it)
- identifying the person who has responsibility for protecting personal information within an organization
- getting informed consent from the individual
- maintaining accuracy and completeness of records
- providing access to the information and a right of correction.

Fair information practices are the cornerstone of most efforts to protect personal information around the world. They form the basis of the

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which were developed by the Organisation for Economic Co-operation and Development (OECD) in 1980 and signed by Canada in 1984. The Guidelines were designed both to protect personal information and to ensure the free flow of information.

These Guidelines have been widely adopted. Their influence can be seen in Quebec's legislation to protect personal information in the private sector. It is also apparent in the laws that govern the public sector federally, as well as in the provinces of British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec and Nova Scotia and the Yukon and the Northwest Territories. New Brunswick is preparing to introduce such legislation shortly.

The CSA Standard

While the current privacy protection regime in the private sector is clearly in need of refocussing, important work has been done in the past few years. In the early 1990s, the Canadian Standards Association (CSA) gathered representatives from the public sector, industries (including transportation, telecommunications, information technology, insurance, health, and banking), consumer advocacy groups, unions and other general-interest groups to discuss the need for a common code to protect personal information in the private sector.

The outcome of the initiative was the development of the Model Code for the Protection of Personal Information, which represents a consensus among all the stakeholders. Based on the OECD Guidelines, the Code is a set of principles for the protection of personal information in the private sector. It addresses two broad concerns: the way in which organizations collect, use, disclose and protect personal information; and the right of individuals to have access to personal information about themselves and to have the information corrected if necessary.

The Standards Council of Canada adopted the CSA Code as a National Standard in 1996, making Canada the first country in the world to adopt such a standard. The Standard demonstrates the continued commitment of participating parties to fair information practices, while providing an instrument that promises to be consumer-friendly, fair, effective and cost-efficient. The result of cooperation among a wide cross section of interest groups, it is truly a remarkable achievement.

The CSA Standard has generated significant international interest. In May 1996, the consumer policy group of the International Organization for Standardization (ISO) passed a unanimous, 25-country resolution in favour of a proposal to develop an international standard on privacy based on the CSA Standard. ISO is

now studying whether there is a need for an international standard to address information privacy, measure privacy protection and ensure global harmonization. If ISO accepts the CSA Standard as the basis for an international standard, Canadian companies that have already applied the principles of the Standard will have a significant advantage.

A few of the organizations that voted unanimously in support the CSA Model Code:

- American Express Company
- Cable Television Standards Foundation
- Canadian Bankers Association
- Canadian Cable Television Association
- Canadian Direct Marketing Association
- Canadian Labour Congress
- Canadian Life & Health Insurance Association
- Equifax Canada
- Fédération nationale des associations de consommateurs du Québec
- Information Technology Association of Canada
- Information Technology Industry Council
- Insurance Bureau of Canada
- Public Interest Advocacy Centre
- The Reader's Digest Association
- Stentor Telecom Policy Inc.

The success of the CSA Standard puts Canada in a good position to move forward from an environment of voluntary codes to a regulated approach to privacy protection. The new legislation will build on the work that has already been done to develop the Standard, as well as the work that various industries have done to implement it. By doing so, the legislation will address two fundamental issues. First, while the Standard provides solid protection, it is only a voluntary instrument, so there is no guarantee that it will be widely implemented. Legislation will ensure that the privacy principles are widely implemented, providing even protection for consumers. Second, as a voluntary instrument, the Standard does not provide for oversight or any way of ensuring effective consumer redress when there is a dispute. Light, flexible and effective legislation will provide the kind of backup that is needed to ensure that, when there are problems, consumers have mechanisms for recourse.

Part 2: Designing Canada's New Privacy Law

The second part of this paper looks at a series of issues that must be addressed in developing legislation to protect personal information in the private sector, and sets out some options for how these issues can be approached. In particular, the new legislation will need to address the four key elements common to all data-protection laws:

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

Throughout this section, the emphasis is on developing a legislative regime that draws on the best features of legislation in other countries and builds on the success of the CSA Standard.

Canada's new legislation should:

1. foster responsible privacy practices on the part of those in the private sector who hold personal information
2. 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
3. be flexible, simple and effective, and consumer-friendly, with enforceable rights and effective means for redress
4. be cost-effective and administratively efficient and not overly burdensome for industry, especially small businesses
5. conform with our international obligations and trade agreements.

Ensuring Protection across Canada

In constructing a model for Canada, one of the fundamental considerations will be how the responsibility for protecting personal information in the private sector should be shared among the provincial, territorial and federal governments.

In Canada, some parts of the private sector are federally regulated, such as the telecommunications and banking industries and interprovincial transportation. Other parts of the private sector, such as health care and education, fall under provincial jurisdiction. Harmonized protection of personal information that covers the entire private sector would be the best way to address the increasing

mobility of information and to guard against the creation of "data havens" or barriers to the free flow of information.

If truly comprehensive privacy protection for all Canadians is to be achieved, then the federal, provincial and territorial governments will have to work closely and cooperatively to ensure a harmonized approach in all jurisdictions. This is vital for interprovincial trade, as well as for international trade.

One possible forum for such cooperation is the Uniform Law Conference of Canada (ULCC), an independent group that promotes the uniformity of legislation across the country. The ULCC began working on a draft Uniform Data Protection Act for the private sector in 1995, and expects to circulate a draft uniform Act for comments in 1998. Once complete, this model could help federal, provincial and territorial governments to develop a harmonized approach.

Other forums being used to work cooperatively on the protection of personal information across all jurisdictions are the Information Highway Ministers' Meetings and similar meetings of Consumer Affairs Ministers. These meetings are good opportunities for Ministers to identify common goals and to commit themselves to working in a harmonized fashion.

Finding Basic Principles

The first question in putting together legislation to protect privacy in the private sector is: What set of principles should the law be based on? Since the same basic set of fair information practices is found in legislation throughout the world, any of these could serve as the basis of the law. It would make sense, however, to build on the consensus that has been achieved around our National Standard. The CSA Standard has been acknowledged in many forums as an improvement over the OECD Guidelines. Principles based on the CSA Standard would help to ensure compatibility with other regimes that have also legislated to a higher standard than the Guidelines, such as Quebec.

The Standard embodies the following 10 fair information principles:

- **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 the Code's 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 is necessary for the fulfilment of those purposes.
- **Accuracy:** Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be 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 personal 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 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 Standard includes an interpretation of each of the 10 principles. There is also a companion workbook that provides more detailed guidance on putting the Standard into practice. These tools make it easy for companies to interpret and implement the Standard.

The CSA Standard has a number of advantages as a starting point for legislation. First, it represents a consensus among key stakeholders from the private sector, consumer and other public interest organizations, and some government bodies. Second, the CSA Standard provides flexibility; it was designed to serve as a model for more specific industry codes. Third, the CSA Standard is technologically neutral; its principles go beyond specific industry applications. Consequently, the Standard will not become outdated as technologies for the collection and storage of information change. Ideal legislation for Canada would build on the successes in voluntary compliance experienced with the CSA Standard while ensuring its rapid, widespread implementation.

If the legislation were to be based on the CSA Standard, a number of questions would have to be addressed.

To begin with, is the CSA Standard, which was drafted as a voluntary instrument, precise enough in setting out legal obligations or would it require further elaboration? Precision and certainty are important aspects of any legislation, because they help ensure that governments, consumers and businesses are clear on their respective rights and responsibilities. Such clarity is especially important when a dispute between an individual and an organization may have legal implications. Provisions of the CSA Standard that may need to be made more precise include when and how personal information may be collected and for what reasons, how long an organization may keep such information, what consent must be obtained for its collection and in what form, and what fees can be charged for copies of records.

The law would also have to specify the exceptional circumstances under which personal information may be disclosed to a third party without the consent of the individual. Sometimes these disclosures do not fall within the purposes for collection as stated by the organization. Such circumstances might include the protection of the health and safety of one or more individuals, emergency situations where it is impossible to obtain the individual's consent, the conduct of medical research, the compilation of statistics, the conduct of lawful investigations, and compliance with a court order.

A second question is: Are there any additional obligations not set out in the CSA Standard that should be included in the legislation? Such obligations could include a duty to report any complaints received to a government body or a requirement to educate members of the public about their rights, or indeed new obligations unforeseen in the original Standard.

A third question is: should some types of information be excluded from the scope of the legislation? For example, Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* does not apply to journalistic material collected, held, used or communicated for the purpose of informing the public.

At a technical level, the obligations and approach of the CSA Standard could be incorporated in law by setting out the basic principles in the statute, with more precise details included in regulations or some other instrument such as sectoral codes. Regardless of how the necessary details were incorporated into law, organizations that use personal information would be required to meet the obligations of the statute.

Sectoral Codes

Many organizations in Canada have already developed privacy codes, and some are upgrading them to meet the CSA Standard. The Canadian Bankers Association, the Insurance Bureau of Canada and the Cable Television Standards Foundation, for instance, have already released codes that conform to the Standard. Other organizations are also working toward this goal.

Sectoral and company codes provide detail and guidance on how legal requirements apply to a specific industry or company. In some ways, these codes are a blueprint for how the law will be reflected in the real-life information practices of the companies that are subject to them.

Many organizations may find that the principles of the legislation are sufficient in themselves, and may not feel a need to develop their own specific codes. This is likely to be the case for many small businesses. Such organizations would simply be required to adhere to the principles set out in the law. Other organizations, however, may prefer to draw on their own expertise to interpret the law as it relates directly to their line of business, and so may see value in developing sectoral codes which would supplement or replace the requirements of the law.

Sectoral codes can be beneficial in a number of ways. First, they allow industries to explore their own needs for personal information and to show their commitment to privacy by imposing discipline on their own practices. This commitment and leadership can help create consumer trust, and they encourage both consumer protection and market leadership. Second, the process of developing a code can help to promote education and acceptance of good information management practices within an organization, thus encouraging staff and management to take an active approach to interpreting and implementing their own information practices. Third, the existence of specific codes facilitates audits by providing a manual of information practices, which can be used as a measuring stick against which to judge the practices of particular companies.

Sectoral Codes in Practice: The Canadian Bankers Association Privacy Model Code

The Canadian Bankers Association (CBA) has been a leader in developing voluntary approaches to protecting personal information. The banking industry developed its first privacy code in 1986, and modified it subsequently on two occasions. Then, over the period 1995–1996, the CBA worked to ensure that its code was consistent with the CSA Standard.

The CBA code has been verified as complying with the CSA Code by Price Waterhouse, and banks are now working individually toward full implementation of the provisions of the code through their own privacy codes.

Copies of the CBA code are available from:

Canadian Bankers Association
Box 348, Commerce Court West
30th Floor
Toronto ON M5L 1G2

Tel.: (416) 362-6092
Fax: (416) 362-7705

Recognition of Sectoral Codes

Should sectoral codes be recognized in the new law? If so, should they be binding, or should they be used only to help guide the interpretation of the principles of the law for specific sectors?

Other jurisdictions have dealt with these issues in a variety of ways. The Quebec law, for example, makes no reference to sectoral codes. Nevertheless, several industry associations with members operating in Quebec have developed such codes for their own organizational purposes.

The United Kingdom law obliges the Data Protection Registrar to encourage the development of codes. These codes aid in interpreting the law, but are not legally binding. The law in the Netherlands makes the Privacy Commissioner responsible for approving codes developed by industry. As in the United Kingdom, these codes are not binding but do give guidance in interpreting the law.

In New Zealand, sectoral codes have the full force of law. A code may be more or less stringent than the principles set out in the law but, once it has been approved by the Privacy Commissioner, it replaces those principles. Developing such codes is a labour-intensive process, but has resulted in a very thorough Code for the Protection of Health Information and one for the use of unique identifying numbers for superannuation.

There are essentially two ways of recognizing sectoral codes in the law:

- Building on the Netherlands approach, industries could be encouraged to tailor codes. Once approved, the codes would be used to guide interpretation but would not be legally binding.
- Following the New Zealand model, approved codes could replace the requirements set out in the legislation and be legally binding.

A further question arises from these options: Who should develop sectoral codes? Having industry develop the codes would avoid placing a huge burden on government overseeing agencies, which generally would be ill-placed to develop specific sectoral guidelines on their own but which are most useful in engaging companies in a dialogue about the adequacy of the finished product. To assist them in developing codes, companies could make use of the growing body of privacy expertise. Alternatively, a government body with privacy expertise could take on the task of developing the codes.

Approval

Once sectoral codes have been written, who should approve them and how?

Legally binding codes clearly require a more rigorous process than codes that would simply provide guidance. Care must be taken to avoid setting up a conflict-of-interest situation whereby a privacy commissioner, for instance, would collaborate on the development of a code and then be tasked with resolving consumer complaints about it.

Regardless of whether or not the codes are binding, they could be approved through a government body responsible for verifying each code to make sure it conforms with the law. This body could then conduct an audit of organizations implementing the code to assess the level of conformity and approve the code. Administrative or legal measures would have to be put in place to ensure that, if the same body had overseeing powers, no conflict of interest would arise. The cost of having such a body approve codes, from the point of view of both government and industry, must be weighed against the possible costs associated with other methods of approving codes.

Non-binding codes could also be verified by either:

- a body accredited as a quality registrar by the Standards Council of Canada, which would conduct an information audit, as is the case now with the process of registering to the CSA Standard; or
- internal or external auditors or other parties with expertise in information management.

Binding codes could also be verified in one of two ways:

- By an accredited registrar. The registrar would recommend that the code be recognized as conforming with the law. A government body or official would receive the recommendation, hold open public hearings, and give the final approval for verification.
- By a government oversight body. Following verification by that body, an approved auditor would conduct an information audit to ensure that the code is being implemented. After the audit, companies could apply for a ministerial exemption allowing them to replace the requirements of the law with their own sectoral codes. There could be provisions for public comment before the code is approved, and passing periodic audits would be necessary to maintain the exemption.

Ensuring Compliance with the Law and Effective Redress of Complaints

Once the basic obligations and the role of sectoral codes have been clarified, their compliance must be assured through an overseeing regime for handling complaints and resolving disputes. Another function of the oversight regime would be ensuring that both the public and the organizations affected by the law are aware of and adhere to its provisions.

Most existing laws for the protection of personal information in jurisdictions around the world establish one central oversight authority, but this varies, particularly in federal states. It would probably make sense to use existing oversight bodies where appropriate, such as the Office of the Privacy Commissioner of Canada.

In designing the most appropriate oversight regime for Canada, there are two primary considerations. The first is the powers needed to adequately oversee observance of the new law and ensure redress. The second is how these powers should be distributed.

It is important to keep in mind that certain kinds of powers, such as ordering fines or restitution when the law is violated, are appropriate to some oversight bodies but not to others. Given appropriate powers and responsibilities, industry associations, existing regulatory and self-regulatory bodies, a privacy commissioner and a federal court or tribunal all could play a role in overseeing privacy protection. In determining who makes final decisions, possible conflicts of interest must be guarded against.

Accountability

The first issue anyone charged with overseeing the new legislation must address is: Are the people and organizations complying with the law? The CSA Standard requires that companies identify an officer within the organization who will be accountable for compliance. This obligation would become binding in the new law. Additional mechanisms could also be

used to ensure compliance with the new law, such as the following examples:

- some kind of registration requirement that organizations state their information management practices, as in the system in the United Kingdom
- some kind of initial audit to ensure adherence to the law
- encouragement, if not a requirement, for organizations to undergo some sort of external review of their information management practices to demonstrate their compliance
- reliance solely on complaints to expose violations
- reliance on a central authority with broad powers to conduct research, write reports, and conduct investigations.

Registration and audit schemes have value in that they help identify problems early on in the implementation process. They also serve to educate staff within an organization. A scheme whereby external review is compulsory could have some drawbacks, however. It may place a heavy burden on small businesses and on organizations that make little use of personal information or of information that is sensitive. It may also be expensive and burdensome to government.

It may be more viable for government to encourage, but not require, organizations to have their information practices audited. In this way, companies could show market leadership and demonstrate a greater commitment to privacy. One way to do this could be by permitting formal registration to the CSA Standard through a body accredited by the Standards Council of Canada. This approach would build on existing mechanisms and current voluntary practices. Companies choosing not to undergo such audits would still have to comply with the law, however.

Another option would be to neither require nor encourage any registration or third-party appraisal of information management practices. In many countries with data-protection laws, compliance is assumed unless a dispute or investigation reveals a problem. A possible weakness of this approach is that it relies heavily on the public to discover abuses, which can be quite difficult in the current climate of sophisticated dataprocessing techniques.

To compensate for this potential weakness, the law could deal with compliance monitoring by empowering a central authority or privacy commissioner to do research, prepare reports on new issues such as new technologies, and perform audits or inspections proactively in addition to responding to complaints. In order for this to be as effective as an upfront registration or audit scheme, there would have to be significant resources committed to this function.

Response to Complaints

The next issue is the handling of complaints. The legislation will give individuals the right to complain and to challenge compliance with any part of the law, affording them a key role in monitoring organizations. By directing the complaint to the company first, a potentially significant burden on the oversight authority is reduced.

Thus, businesses will have the opportunity to learn from their mistakes and show market leadership in correcting them and developing consumer trust.

Businesses should take an active role in monitoring their own practices and should cooperate with consumers in resolving problems. To help track compliance with the law, companies could be required to report any complaints they receive to an oversight body.

In the event that an individual is not satisfied with an organization's accountability mechanisms, however, there must be a second avenue for redress. The oversight body should have a range of powers to investigate and to attempt settlement. It should be able either to reach final judgment on the dispute or to empower the individual to move on to a court for final judgment.

Several questions arise:

- What powers are needed to investigate possible cases of non-compliance and resolve disputes? These could include the power to receive and initiate complaints, investigate information practices, conduct or demand an audit, examine witnesses, require testimony and order the production of documents, act as a mediator in disputes, and issue recommendations or binding orders.
- What powers are needed to address violations of the law and compensate individuals who have been harmed? These could include powers to order fines or restitution, award damages, order corrective action, demand full registration to the CSA Standard if the law does not already require it, order periodic audits, restrict the use or transfer of personal information by non-compliant companies, and publish the details of violations.

Oversight Agencies

An important aspect of any legislation to protect privacy in the private sector is the mechanism by which effective oversight of the law is ensured. There are a number of agencies which could be used to perform this function. For example, in Canada, banks, cable companies, airlines and other industries are already subject to the authority of regulatory agencies. These agencies have expertise in these industries, so it would make sense to use existing regulatory bodies in some capacity for overseeing privacy protection. Care

should be taken, however, to ensure that taking on this additional capacity would not weaken the coherence of a harmonized regime or result in differing interpretations of the legislation.

There may be value in distributing the oversight powers among a number of agencies, which could include businesses, industry associations and existing regulatory bodies in conjunction with a privacy commissioner or a special court or tribunal. The distribution of powers among these agencies could be determined on the basis of existing practices, cost, conflict of interest and recognition of the fundamental rights of the individual to effective redress.

The first step in any normal redress procedure could be consideration of the complaint by the company involved. If the problem is not resolved, the complaint could then go to the privacy commissioner, who could mediate or refer the complaint back to the company for mediation through industry-led mechanisms, assuming these have not already proven unsuccessful. Such mechanisms might include an industry ombudsman or some other body. In several sectors, such as banking or telecommunications and broadcasting, regulatory bodies could play a role.

Where disputes deal with systemic issues or where complainants do not feel that they can obtain satisfaction through industry-led processes, there may be a role for the privacy commissioner, a special court or tribunal, or both. Extending the mandate of the existing Privacy Commissioner would require additional resources, but some of the functions normally associated with the Commissioner could be distributed among the various other parties.

A privacy commissioner with a mandate to monitor compliance, make recommendations about sectoral codes and issue special reports on new technologies or practices might be compromised in having to make a final binding judgment on a complaint involving activities he or she had overseen or audited. Several other countries have set up special tribunals for hearing cases to avoid this situation. Does this option have merit for Canada?

Public Education

Legislation to protect privacy in the private sector would be most effective if it included measures that address emerging privacy issues proactively through consumer education. In a light regulatory framework which does not impose a heavy burden on industry, consumer education is especially important to ensure that citizens are well informed about their privacy rights and are vigilant in protecting them.

The following issues need to be considered:

- Where should responsibility for public education lie? The law could make the privacy commissioner solely responsible, or it could divide the responsibility with businesses, industry associations and regulatory bodies.
- Should the privacy commissioner be encouraged or required to provide advice to individual companies on privacy issues? This could be done informally or in conjunction with compliance audits. In many countries, including Canada, privacy commissioners provide advice to organizations about their information management practices and about privacy issues more generally, through both informal and formal channels. This gives the commissioners an opportunity to influence systems at the design stage, and helps to raise awareness of and sensitivity to privacy issues. Providing this kind of advice must not, however, interfere with the commissioners' ability to receive complaints or conduct investigations.
- Should the law require privacy impact assessments of new information technologies? If so, when and by whom? New information technologies can either erode or preserve privacy. The legislation could play a role in promoting the use of those that enhance privacy by requiring privacy impact assessments of all new information technologies where appropriate. These assessments would focus on how the new information technology protects personal privacy, whether it provides more or less protection than previous technologies for the same purpose, and whether it provides options, such as paying for services anonymously, for individuals who demand greater privacy.

Striking the Right Balance for Made-in-Canada Legislation

The challenge facing Canadians is to find a balance between the needs of business for access to the information necessary for functioning in a knowledge-based economy and the rights of individuals to privacy and security of personal information. Collectively, we must ensure that technological innovations do not become intrusions on these economic needs and fundamental rights. Because the information economy is still in its infancy, Canadians now have the opportunity to define and design the kind of system we want to establish for safeguarding information privacy in the private sector. Rapid technological advances, however, demand that we formulate a legislative framework before many of the issues discussed in this paper move beyond our control.

Even in dealing with such a complex issue as protection of personal information in a digital economy and society, it is possible for citizens, businesses, and governments to reach a common understanding and to find a solution which addresses the needs of all stakeholders. The CSA Standard is an excellent case in point. This discussion paper will encourage public debate on the issues it lays out, and submissions in response to the paper will contribute to the formulation of a common Canadian approach to the protection of personal information in the private sector.

Part 3: Your Turn

This paper has raised a number of specific questions with regard to the form that federal legislation to protect privacy in the private sector should take. In considering these questions, it is important to make sure that the new law strikes the right balance between the business need to gather, store, and use personal information and the consumer need to be informed about how that information will be used and assured that the information will be protected. Achieving this balance is a key element in fostering an environment that will enable Canada to emerge as a world leader in electronic commerce.

Industry Canada and Justice Canada look forward to receiving your comments on the questions raised throughout the paper. For your convenience they are listed below, along with some related questions that will also need to be addressed as we develop legislation.

Obligations

1. Is the CSA Standard the base from which to start in drafting legislation? Is it precise enough in setting out obligations or do some obligations require further elaboration? Are there any additional obligations not set out in the CSA Standard that should be included in the legislation?

2. Under what circumstances should the law permit disclosure of personal information to a third party without the consent of the individual? What conditions should apply?

3. Should sectoral codes be recognized in the new law? If so, should they be binding? Or should they be used only to help interpret the principles of the law for specific sectors? Who should develop and approve them?

4. Should some types of information be excluded from the scope of the legislation? If so, in what circumstances?

Powers

5. Do you favour start-up obligations such as a registration scheme to ensure compliance with the law? If so, which approach do you favour? Who should be responsible for overseeing privacy protection?

6. What powers are needed to investigate possible cases of non-compliance and resolve disputes about the terms of compliance?

7. What powers are needed to address violations of the law and compensate individuals who have been harmed?

8. Should there be powers to conduct independent research and proactive investigation/inspection of an organization's practices and to write reports?

Distribution of Powers and Responsibilities

9. Should a central oversight authority be established to oversee the implementation of the new legislation, and if so, what powers should it have? Should this role be added to the responsibilities of the federal Privacy Commissioner or some other body?

10. Should a tribunal be established, or should a higher court be given the task of issuing binding decisions on complaints?

11. What use should be made of existing industry regulators or of industry-led, self-regulatory mechanisms? How can such bodies be set up to satisfy business, consumer and government expectations?

12. How should responsibilities for public education be assigned?

13. Should the law require privacy impact assessments of new technologies? If so, when and by whom?

Cooperation

14. How should responsibilities for protecting personal information in the private sector be shared among the provincial, territorial and federal governments?

15. What forums, in addition to those discussed in the paper, would be useful in harmonizing the protection of personal information in all jurisdictions in Canada?

Thank you for your contribution to this consultation process. Please have your responses in by March 27,1998. Send your comments to:

Helen McDonald
Director General, Policy Development
Task Force on Electronic Commerce
Industry Canada
20th Floor, 300 Slater Street
Ottawa ON K1A 0C8
Fax: (613) 957-8837
E-mail: privacy@ic.gc.ca

Annex: Resources

A number of publications are referred to in this paper. Many of them are available electronically, and paper copies can be obtained by contacting the Industry Canada Task Force on Electronic Commerce:

Tel.: (613) 990-4255
Fax: (613) 957-8837
E-mail: privacy@ic.gc.ca

CAN/CSA-Q830-96 Model Code for the Protection of Personal Information (the CSA Standard) is available at: *http://www.csa.ca/83002-g.htm*

The 1980 ***Guidelines on the Protection of Privacy and Transborder Flows of Personal Data***, developed by the Organisation for Economic Co-operation and Development (OECD), an abridged version are available at: *http://www.oecd.org/dsti/sti/it/secur/ prod/PRIV-EN.HTM#3*

The 1995 European Union ***Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*** is available at: *http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html*

The federal ***Privacy Act*** is at: *http://canada.justice.gc.ca/stable/EN/Laws/Chap/P/P-21.html*

Two excellent sources of further on-line information about privacy are:

The **Office of the Privacy Commissioner of Canada**, at: *http://infoweb.magi.com/~privcan/*

Media Awareness Network, at: *http://www.schoolnet.ca/medianet*

Glossary of Terms

A number of terms are used throughout this paper which have a specific meaning within the context of privacy and the protection of personal information. They are listed below.

Electronic Commerce: All commercial transactions, involving organizations and/or individuals, based on the processing and transmission of digitized information.

Information Privacy: A subset of privacy, it involves the right of individuals to determine when, how and to what extent they will share personal information about themselves with others. Protecting information privacy involves protecting personal information.

Personal Information: Any information about an identifiable individual that is recorded in any form, including electronically or on paper. Some examples would be information about a person's religion, age, financial transactions, medical history, address, or blood type.

Privacy: Most often defined as the right to be left alone, free from intrusion or interruption, privacy is an umbrella term, encompassing elements such as physical privacy, communications privacy, and information privacy. Privacy is linked to other fundamental human rights such as freedom and personal autonomy.