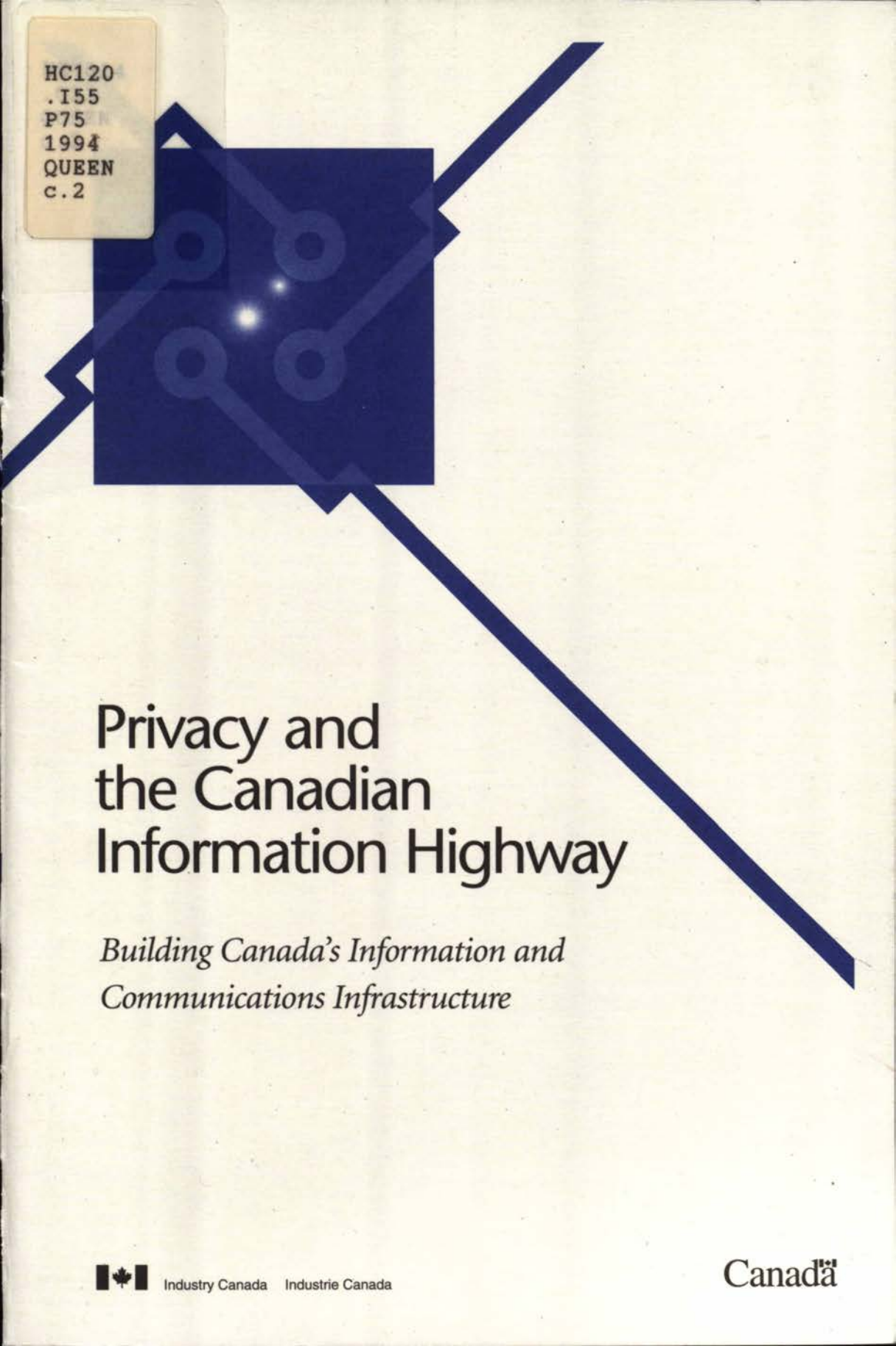


HC120  
.I55  
P75  
1994  
QUEEN  
c.2



# Privacy and the Canadian Information Highway

*Building Canada's Information and  
Communications Infrastructure*



Industry Canada Industrie Canada

Canada

HC  
120  
.T55  
P75  
1994  
Queen  
c.2



INDUSTRY, SCIENCE AND  
TECHNOLOGY CANADA  
LIBRARY

OCT 26 1994

BIBLIOTHÈQUE  
INDUSTRIE, SCIENCES ET  
TECHNOLOGIE CANADA

# Privacy and the Canadian Information Highway

Communications Development and Planning Branch  
Spectrum, Information Technologies  
and Telecommunications Sector  
Industry Canada  
October 1994

*Privacy and the Canadian Information Highway* and many other Industry Canada documents are available electronically on the Internet computer network at [council@istc.ca](mailto:council@istc.ca).

Anyone with the ability to use Anonymous file transfer (FTP), Gopher or the World Wide Web can access these documents. Below are the Internet addresses:

**Anonymous file transfer (FTP)**

[debra.dgbt.doc.ca/pub/isc](ftp://debra.dgbt.doc.ca/pub/isc)

**Gopher**

[debra.dgbt.doc.ca port 70/Industry Canada Documents](gopher://debra.dgbt.doc.ca:70/Industry%20Canada%20Documents)

**World Wide Web**

<http://debra.dgbt.doc.ca/isc/isc.html>

Additional print copies of this discussion paper are available from:

Distribution Services  
Industry Canada  
Room 208D, East Tower  
235 Queen Street  
OTTAWA, Ont  
K1A 0H5  
Tel.: (613) 954-5716  
Fax: (613) 954-6436

A companion document, *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure*, is also available from this address.

For information about the contents of this discussion paper and the consultation process, contact:

Information Highway Advisory Council Secretariat  
Room 640, Journal Tower North  
300 Slater Street  
OTTAWA, Ont.  
K1A 0C8  
Tel.: (613) 990-4268  
Fax: (613) 941-1164

© Minister of Supply and Services Canada 1994  
Cat. No. C2-229/1-1994  
ISBN 0-662-61370-8  
SIT PU 0025-94-03



# Contents

<b>Preface</b>	1
<b>Introduction</b>	3
<b>1. What Is Privacy?</b>	5
<b>2. Privacy Issues for the Information Highway</b>	6
Transactional Data and Personal Profiling	6
Transactional Security and Individual Identification	7
Identity Cards and Single Identifier Numbers	7
Monitoring and Surveillance	8
Intrusion	9
<b>3. What Privacy Protection Now Exists in Canada?</b>	10
Protection in the Public Sector	10
Protection in the Private Sector	11
<b>4. How Have Other Countries Protected Privacy?</b>	13
<b>5. Possible Approaches for Canada</b>	15
Legislation and Regulation	15
Voluntary Codes and Standards	16
Technological Solutions	17
Consumer Education	18
<b>6. Public Comment</b>	19
<b>Annexes</b>	20
A — Chronology of Background Events	20
B — The OECD Guidelines and the Draft CSA Privacy Standard	22
C — Telecommunications Privacy Principles	23



# Preface

The information highway of the future might be more accurately described as the advanced information and communications infrastructure that is essential for Canada's emerging information economy. Building on existing and planned communications networks, this infrastructure will become a "network of networks," linking Canadian homes, businesses, governments and institutions to a wide range of interactive services, from entertainment, educational and cultural products to social services, data banks, computers and electronic commerce as well as banking and business services.

Industry Minister John Manley in March 1994 created a national Information Highway Advisory Council to assist the federal government in developing and implementing a strategy for Canada's information highway. It is the council's responsibility to provide the necessary advice and guidance to government on the variety of issues raised in the government's discussion paper *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure* (Ottawa: Minister of Supply and Services Canada, 1994), prepared by Industry Canada. Within this framework, the council will be examining how an advanced information infrastructure will improve the growth and competitiveness of Canadian businesses; how to ensure universal, affordable access to essential services for all Canadians; how to develop an appropriate balance between competition and regulation; and how to promote the development and distribution of Canadian culture and content.

Five working groups have been established by the advisory council to cover the following broad areas of interest: Access and Social Impact; Canadian Content and Culture; Competitiveness and Job Creation; Learning and Training; and R&D, Applications and Market Development. The working groups and the council meet on a regular basis and are engaged in a variety of activities to explore the issues, consult with the public and make recommendations to the federal government.

To seek the public's views and to raise the level of debate on privacy issues, Industry Canada is releasing the discussion paper *Privacy and the Canadian Information Highway* in cooperation with the advisory council. It is the first of several discussion documents to be released by Industry Canada on social, economic and technology policy issues. Written submissions and/or comments are invited from all interested parties on the various options and approaches presented or on any portion of this discussion paper.

Submissions should be addressed to:

Parke Davis, Director General  
Information Highway Advisory  
Council Secretariat  
Room 640, Journal Tower North  
300 Slater Street  
OTTAWA, Ont.  
K1A 0C8

All submissions must be received on or before December 23, 1994 (see *Canada Gazette*, Part I).

## PREFACE

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  
2nd Floor, Journal Tower South  
365 Laurier Avenue West  
OTTAWA, Ont.  
K1A 0C8

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

# Introduction

Businesses, public institutions and governments gather, store, transmit and exchange vast amounts of personal and business-related information both in paper format and electronically. The shift to computer-mediated interaction and the interconnection of networks will increase the amount of personal and transactional information that can be assembled into comprehensive profiles of individuals. In many cases, these records can be sent across national borders, sold or reused, or integrated with other data bases, for purposes unrelated to those for which the information was originally collected, without the consent of or compensation to the individual from whom the information was obtained. There is no question that the ability to access, repackage and resell information can benefit individuals and firms, and create new employment opportunities. On the other hand, it raises concerns among the general public, the business community and government alike about privacy protection and the security of sensitive information.

Public surveys of Canadians have consistently revealed a remarkably high level of concern over the issue of privacy. The 1992 Canadian Privacy Survey by Ekos Research Associates Inc. found that 92 percent of the 3 000 Canadians interviewed believed privacy to be an important issue, and that 60 percent believed they have less personal privacy now than a decade ago. Respondents also

indicated they would be more at ease with others using their personal information if they had control over this information, knew their privacy rights were protected and knew government exercised some form of oversight or monitoring of these activities. A 1994 Gallup Canada survey for Andersen Consulting revealed that over 80 percent of the Canadians polled expressed concern about the personal information about them that might be collected by companies through the information highway. These studies suggest a pervasive belief that personal privacy is under siege from a range of technological, commercial and social threats and that something must be done about it. What is the role that government, businesses and individuals should play? What concerns must be addressed? What options are available?

Under the Canadian Constitution, the protection of privacy is a shared jurisdictional responsibility of the federal and provincial governments. In fact, Canadians are only partially protected by a combination of federal and provincial legislation, and voluntary codes set by government and the business community. The adequacy of Canada's current legislative framework for privacy protection is reviewed briefly in this paper, as are recent efforts, both federal and provincial, to broaden and enhance this framework to meet new privacy concerns.

## INTRODUCTION

In the "network of networks" world that is now emerging, Canada forms a part of the international "information grid" or "global village." As a sovereign nation, Canada has international commitments to a variety of treaties and conventions; as a trading nation and as a leader in communications technology and services, Canada has an interest in how other nations solve the privacy challenges facing us now. This paper also outlines Canada's participation in international organizations concerned with privacy protection and the efforts of some of our trading partners in this area. Finally, several approaches are proposed to strengthen personal privacy and data protection in Canada.



# 1

## What Is Privacy?

Privacy is usually defined in two ways: the right to be left alone, free from intrusion or interruption, and the right to exercise control over one's personal information.

We Canadians value our right to live in peace, undisturbed by others. It is the right to solitude, to anonymity, to share our time with those we choose, and to define our own space and boundaries. This concept of privacy encompasses a broad range of issues that go beyond the acquisition and dissemination of personal information. While the *Canadian Charter of Rights and Freedoms* does not contain a specific right to privacy, it does guarantee an individual in his or her dealings with government the right to life, liberty and security of person, and the right to be secure from unreasonable search and seizure. Many privacy experts, however, would question the effectiveness of the protection available under the Charter.

Personal data protection has been defined as the claim of individuals to determine when, how and to what extent information about them is communicated to others. Data protection is an aspect of privacy protection that involves control over the collection, storage, accuracy, use and dissemination of personal information.

The high degree of mobility of modern Canadian lifestyles brings us into contact with a great many people who may not know us personally, except through various types of information we provide about ourselves. In travelling, shopping, obtaining services, driving our vehicles, and communicating from different locations, there is a need for us to provide secure identification of who we are and what we are entitled to receive. Service providers of all kinds require and ask for detailed information that will verify our identity and confirm our ability to pay. At the same time, these details and the data trails left by electronic transactions can be used to predict future marketing opportunities and thus increase the incentive to store this personal information in data bases. The exchange and marketing of personal information is flourishing, and it is increasingly taking place across national borders. As a result, data protection is becoming the most critical component of privacy protection.

# 2

## Privacy Issues for the Information Highway

### ***Transactional Data and Personal Profiling***

Transactional data gathering will become much easier in a computer-mediated and networked world. The great strides in computing capacity, the linking of so many businesses by electronic payment systems, and the meshing of sales and ordering data bases have revolutionized the relationship between consumers and the producers of goods and services. With "just-in-time" supply management, producers manufacture and ship goods to warehouses and suppliers in direct response to the data transmitted from the point-of-sale terminals of their clients.

Wholesalers and retailers increasingly are plugging into the chain. The linking of an individual to a particular purchase is merely one more segment of the chain, which facilitates direct marketing and market analysis. Most people may be aware that a credit card company could be selling their transactional data to vendors of products, but they might consider this a reasonable cost of doing business with a huge and reliable credit company, and one outweighed by the benefits. In the new networked environment, every business — large or small, reliable or not — will have the capacity

to generate information files on its customers or to purchase customer data bases from other sources. What is the appropriate balance between the social and commercial benefits of such advanced technologies and the risks they bring to individual privacy? What controls or safeguards should be placed on the use and reuse of this information?

The information highway holds enormous potential to easily compile profiles of individuals' needs, lifestyle habits or purchase choices. This could have negative consequences if such profiles are used to deny opportunities to people without their knowledge. Data base storage and information cross-matching can be used to make decisions about individuals, affecting the terms and conditions of access to a variety of products, services and employment opportunities. This capability could further stigmatize the vulnerable — such as those who are ill, elderly or unemployed, or those who are seeking welfare, health care or citizenship — limiting their chances and curbing the gains we have made in equity and human rights in our society. In a highly competitive job market, where thousands of people send in résumés for



even modest jobs, what kinds of data base screening are we prepared to accept? How can unsuccessful job candidates ensure that they were not passed over because of erroneous information that appears on their records? Should organizations be required to notify individuals of their information holdings and provide no- or low-cost access to these files for verification or correction? Should there be time limits on the storage of information?

Provision of new services such as video on demand, and electronic magazines and catalogue services on the highway will permit the collection of an ever wider range of information regarding one's interests and choice of entertainment and reading material. Is some form of regulation needed to limit storage, access and use of such detailed data? Is it safe to permit such systems to gather information about our habits, even for benign purposes? How can individual privacy rights be protected during the different steps of the information collection, storage and exchange processes? Should informed consent be required for the different information activities and transactions an organization can undertake using personal information?

### ***Transactional Security and Individual Identification***

While encryption or encoding can secure the content of the electronic message, verifying the identities of the sender and the receiver is an equally critical element of privacy. This is especially true for financial and commercial information exchanges or for sending sensitive information. Increasingly, ordinary consumer transactions are not conducted in person, but through a variety

of means, such as telephones, faxes or catalogue orders. Present methods of authentication and payment arrangements require various kinds of personal information that are not easily known by others, ranging from one's credit card number to the maiden name of one's mother. The extension of these commercial transactions at the consumer level to the terminal in the home poses new challenges. How can one verify a person's identity and/or credit worthiness for electronic orders or requests for delivery of medical records? Will present identification procedures continue to be adequate on the information highway? Would other methods, such as digital signatures, prove more secure?

### ***Identity Cards and Single Identifier Numbers***

Another aspect of the privacy debate is the issue of identity cards. New "smart card" technologies afford organizations the means of going beyond the limited information currently stored in magnetic strips to the enormous storage capacity of embedded chips. Detailed information or even pictures of the individual could be encoded on the card, or the data linked to a biometric identifier such as a thumbprint or retinal scan. With the current rates of fraud in card-based authorization systems — be they credit, phone or medical benefits cards — there is growing pressure to move to a more reliable system of identification. Privacy advocates, however, fear the potential of such cards to facilitate unacceptable levels of data matching, or the creation of a society in which it will be mandatory to carry identification documents on one's person at all times. In the face of strong public support for decreasing fraud in our social programs,

where is the line between responsible administration of programs and services, and unacceptable loss of individual liberties and privacy? A single numerical identifier increases the capability to amass and cross-match personal information. Should there be limits on such identifiers?

In the field of health information, privacy is a sensitive issue. Doctors, clinics and hospitals, insurers and governments, epidemiologists and researchers are motivated by differing interests with respect to health records, and may want access to lifelong data for legitimate purposes. But individuals, also legitimately, fear the abuse of this information by benefit providers or employers. In a Quebec trial use of a smart card for medical services, the information stored on the card was sequestered into four quadrants, with each service provider (such as a pharmacy) having access only to the information required. This solves one privacy problem because all players in the medical system are unable to access the complete range of patient data. However, the more fundamental issue of maintaining cradle-to-grave records through advances in technology remains a problem where privacy protection is not comprehensive.

## **Monitoring and Surveillance**

Lifestyles, working patterns and business transactions will be transformed as computing and network power enter every home and business. While each information technology has different capabilities, they all contribute to an unprecedented capacity for surveillance of every man, woman and child, whether as customer, student,

employee, patient, taxpayer or recipient of government services.

One of the most widely used applications on computer networks is electronic mail. The efficiency and convenience of this new information system have brought instant popularity in both commercial and social settings. Should employee e-mail be treated as a private letter, or as company property and therefore available to be read by a system operator or by a supervisor? Should these systems be designed to allow for easy encryption or encoding of the messages, to protect against casual forwarding and broadcasting of sensitive messages? Just as conventions and etiquette have been developed for the handling of personal and business correspondence over the centuries, should these norms be adapted to our new electronic environment?

Teleworking or working at home also brings a risk of increased surveillance. Managers may want to measure the productivity of employees who work at home by counting keystrokes, timing phone calls or wiring video cameras to the network. These techniques are already in use in some specialized areas of the work force. What limits, if any, need to be imposed on such monitoring? Is government regulation required, or will encouraging good behaviour and fair contracting practices suffice?

The information highway promises to support banking, teleworking, utility and appliance management, and other monitoring activities in the home. This raises serious questions not only about security of data on the network, but also about security in the home, whereby an intruder could enter and force the homeowner to withdraw money or to



credit another account through the home computer system. Home surveillance and protection systems offer security from burglary and fire, but how intimate should such systems be? Must there be a video data stream of every doorway and accessible window in our house sent to a security company or the police department? What controls should be put in place for the collection, use, availability and possible resale of information gathered about our use of different services in the home?

Another category of personal information is provided through satellite technology for global mobile telephone coverage. There will soon be available a unique individual telephone number that travels with each person, from the workplace to the home, the cottage, friends' apartments or businesses and other trips. Local cellular systems and other new personal communications services will have a similar capacity to track phones, using conventional radio and microwave technology. The gains in convenience are obvious, but the catch is that the computer must know exactly where each person is at all times. Privacy advocates want to know who will control the information about our whereabouts, how long it will be kept, and how far this "electronic leash" will extend. How should the different interests of employees and employers be balanced in this and similar forms of monitoring?

## ***Intrusion***

Citizens may also want to be protected from unwanted communications as a result of purchasing goods on the electronic highway. Disturbances or intrusions by telemarketers or targeted advertising mail is a privacy nuisance that concerns many Canadians. There is already "junk" fax, with solicitations over our fax machines for everything from coffee service to holiday trips. Should controls target marketing schemes that result from separate or related purchases — for instance, junk e-mail that follows a purchase of a Caribbean holiday with offers for a next trip? If so, how? What rules should govern the collection and use of information about what people buy or other personal information transactions? How should these rules be balanced with the opportunity to be made aware of goods or services that people might want and need?



# What Privacy Protection Now Exists in Canada?

Over the past 20 years, the history of data protection legislation in the developed world has reflected the effort to balance what democratic countries perceive as the fundamental right of privacy and the need for government and business to obtain personal information that allows individuals to participate in a complex global society (see Annex A). Codes of fair information practices began to emerge, which limited the collection of information and established the right of the individual to access his or her own data, challenge its accuracy and correct any inaccuracies. During the 1970s, the Organisation for Economic Co-operation and Development (OECD) recognized the need to address the issue of personal privacy in the context of the growing transborder flow of information. Member countries, including Canada, started work on a set of guidelines. In 1981, the OECD released its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (see Annex B). Canada and other member countries adopted the Guidelines and indicated that they would be addressing privacy issues, either by passing legislation that incorporated the principles or by putting in place voluntary systems that would give force to them.

## ***Protection in the Public Sector***

Canada employs a mixture of legislation and voluntary codes to protect privacy. Data protection legislation protects personal information held by governments at the federal level and at some provincial and municipal levels. Based on the OECD Guidelines, the federal *Privacy Act* of 1982 protects information held by the federal government. The Office of the Privacy Commissioner was created to monitor the federal government's collection, use and disclosure of its clients' and employees' personal information, and its handling of individual requests to see personal records. In their annual reports to Parliament, Privacy Commissioners have not limited their comments to data protection within the federal government, but have reported on privacy trends across Canadian society. The cause of privacy protection has benefited greatly from these activities.

Some of the provinces have followed suit and have passed comprehensive legislation, starting with Quebec in 1982, Ontario in 1987, Saskatchewan in 1991, British Columbia in 1992 and Alberta in 1994. Nova Scotia introduced a privacy bill for the provincial public



sector in 1993. The powers of the various provincial commissioners or ombudsmen vary. For example, the British Columbia Commissioner can make binding orders, while the Ontario Commissioner makes recommendations. Only the Quebec Commissioner has jurisdiction over the private sector, with the power to impose fines for non-compliance of up to \$20 000.

In Quebec, the issue of privacy has been addressed differently, partly because the Quebec *Civil Code* contains a specific and detailed right of privacy that covers private as well as public information holdings. Quebec has gone further than any other province by passing legislation that protects all personal information held by both the public and the private sectors. This legislation came into force in January 1994. It is one of the first data protection laws of its kind outside Europe, and has already had the effect of encouraging national operations to harmonize to the standard of data protection that must be met in Quebec.

### **Protection in the Private Sector**

Apart from this effort in Quebec, the rapidly expanding use and management of personal information in the private sector is virtually unregulated in Canada, although there have been attempts in specific sectors to voluntarily set and implement fair information or privacy codes. These codes attempt to define boundaries and establish guidelines for personal privacy protection in order to achieve a balance between social and economic benefits, and an individual's right to control over his or her personal information.

The Canadian Direct Marketing Association, for example, has a voluntary code that offers consumers a chance to "opt out" or refuse to let their data be passed on or sold to other companies, and enjoins its members to make their best efforts to help consumers find out where erroneous information may have crept into their files.

The banking sector has had a privacy code since 1991, although the code and its implementation have fallen short of the expectations of privacy advocates, largely on the issues of client access to personal information and the amount of information required for granting credit. In public hearings in 1993, the Canadian Senate explored draft regulations that would address banking privacy concerns, should the Minister of Finance decide in the future that there is a need to regulate in this area. There has been no formal call, however, to move on this proposal.

The telecommunications sector has a mixture of a voluntary approach and regulation. The introduction of caller identification service, which displays the telephone number of the person calling, was criticized by a broad coalition of concerned citizens — from women's shelters to seniors' groups — for its inherent infringement on privacy. Telephone companies were eventually required by the Canadian Radio-television and Telecommunications Commission (CRTC) to offer free per-call blocking, and line blocking for those with particular needs. Around the same time, the privacy of cellular and mobile phones received widespread media attention after the private conversations of public figures were recorded using electronic scanners. In response to these

and other concerns, such as the proliferation of telemarketing and junk fax, the federal government announced a set of Telecommunications Privacy Principles (see Annex C) in December 1992. These principles were designed to encourage awareness of privacy concerns within the industry and to promote a self-regulatory approach. They reinforced the rights of individuals to control their personal information and to be made aware of the privacy implications of new communications and information technology products and services. Although the Telecommunications Privacy Protection Agency, which was proposed to oversee the implementation of these principles, has never materialized into an active force, the principles have influenced the development of voluntary codes within the telecommunications sector.

The new *Telecommunications Act*, which came into effect in October 1993, provides the CRTC with enhanced powers to protect the privacy of individuals and to regulate unsolicited communications. The government also introduced amendments to the *Criminal Code* and the *Radiocommunication Act*, which came into effect in August 1993, forbidding the divulgence of intercepted radio-based telephone communications.

In addition to these sector-specific initiatives, Canada is experimenting with a more inclusive national model code. In the fall of 1990, the Canadian Standards Association (CSA) initiated the development of a national privacy standard that could be applied across all sectors and all provinces. Several federal departments, key private sector players and various consumer representatives are participating in this initiative, and a draft code is expected to be available for public comment late in 1994. With a standards-based approach to data protection, privacy could be addressed during the development of new information and communications technologies, and could be promoted with our trading partners internationally. A national standard for data protection developed in Canada could be included as an element in the International Organization for Standardization's quality management standards (ISO 9000 series), increasing the likelihood that large corporations would treat the management of personal data in the same way they do security, clean room facility management and other quality control mechanisms.



## 4

## How Have Other Countries Protected Privacy?

The European approach to privacy favours omnibus data protection regulations that apply to both the public and private sectors, and are overseen by independent data commissioners.

Countries whose histories have made them sensitive to data protection issues, such as Germany, France, Austria and Sweden, passed laws in the 1970s and, by the end of that decade, there was sufficient imbalance of protection in Europe that the Council of Europe began to discuss a Convention that would bind member countries to producing similar legislation. The OECD developed its Guidelines in 1981 in order to provide the same kind of harmonization among its member states, fearing that the disparity in protection of privacy rights would cause countries with data protection to block the flows of data to those without it. By the end of the 1980s, many European countries had still failed to produce data protection legislation, even though they were obliged by Convention 108 of the Council of Europe. The Commission of the European Community, concerned that data commissioners might block data transfers between countries and thus hinder the development of a single European common market, decided to act.

In 1990, the Commission of the European Community released two draft data protection directives, which, if passed by the European Parliament, will have the force of law. The first was a general directive applying to all personal data, computerized or in manual files, which banned data flows to countries without adequate protection. The second was a tightly modelled directive on privacy in telecommunications, which dictated the precise response member countries and trading partners should take to the intrusions posed by caller identification, cellular and speaker phones, and call detail recording. Response to this initiative was swift, with many businesses and member countries opposed to various aspects of the directive. In 1992, the main directive reappeared with greatly reduced extraterritoriality, and a later version is expected to be passed by the end of 1994.

In contrast, the United States has tended to rely on voluntary codes of practice and sectoral legislation. In 1970, the U.S. passed the first *Fair Credit Reporting Act*, recognizing that the detailed profiling necessary for credit activities must be balanced by opportunities for consumers to examine

## HOW HAVE OTHER COUNTRIES PROTECTED PRIVACY?

their files and correct errors. The federal *Privacy Act* was passed in 1974 to protect the privacy of individuals with respect to information contained in federal government records that was likely to be released under the new *Freedom of Information Act* (FOIA). However, the emphasis was clearly on the FOIA, and there was no independent oversight of the *Privacy Act*. In response to scandals in the credit business, the United States is revising its fair credit reporting legislation.

The United States is also taking a fresh look at privacy in the context of its National Information Infrastructure (NII) initiative, which is similar to Canada's efforts to seek advice on what the future information highway should be. It has struck a task force to look solely at privacy issues. The Working Group on Privacy of the NII Task Force has tabled privacy principles for comment, but the oversight mechanisms are as yet unspecified. The National Telecommunications and Information Agency, the arm of the Commerce Department responsible for policy advice on the NII, has issued a call for comment on the implications for privacy of new telecommunications services, with a discussion paper exploring some of the issues in transaction-generated information.



# Possible Approaches for Canada

Most Canadians doubt their ability to protect their privacy, and see the role of protection as a government responsibility or a joint government/business partnership. Undoubtedly, the development of the information highway will continue to raise these issues and the demand for action.

Possible approaches to privacy protection include legislation, the advancement of a national voluntary privacy standard, the promotion of privacy protective technologies such as encryption and smart cards, and consumer education. Canada may need all of these approaches.

## ***Legislation and Regulation***

Protection of the enormous information holdings of governments, including medical, welfare, tax, immigration and police records, exists at the federal level and in the provinces of Quebec, Ontario, Saskatchewan, Alberta and British Columbia. The quality of coverage varies from jurisdiction to jurisdiction and, when information travels, it is not always clear which law applies. Reflecting this environment in its 1993-94 annual report, the Office of the Privacy Commissioner described Canada's privacy protection as a patchwork of public and private initiatives that address privacy in a piecemeal

fashion. The commissioner called for "national privacy legislation to establish the principles and framework" for both business and government. There is no doubt that both provincial commissioners and governments have recognized these problems too, and it may be time to initiate a dialogue to work toward solutions.

Although federal legislation may well be desirable to provide uniform protection and rights across Canada, the division of authority between federal and provincial jurisdictions appears to preclude this from happening. The federal government has the power to regulate industries such as telecommunications, transportation carriers and banks. The provinces, however, have responsibility for privacy protection in areas such as individual transactions between consumers and the retail industry. By amending existing sectoral legislation, the federal government could create privacy protection requirements in each sector it regulates. Another possible approach would be to extend the federal *Privacy Act* to all sectors of the marketplace within federal jurisdiction. Since this might further exacerbate disparities between regulated and non-regulated entities, it would make sense for jurisdictions to work together toward a common set of rules that could be applied in all sectors.



Federal legislation would respond to the expressed desire of Canadians for a government oversight role in consumer protection. It could also serve to initiate a dialogue for improved privacy protection at the provincial and territorial level. A complementary federal and provincial framework could address such shared concerns as the potential for interprovincial trade barriers caused by differing privacy protection requirements and practices among provinces and territories. It would have to address the need for a level playing field between competing businesses and for consumers coast to coast. The private sector currently faces different regulatory regimes. For example, the privacy protection clauses of the *Telecommunications Act* apply to federally regulated carriers, but not to telecommunications resellers and information service providers. The cost of meeting differing standards is passed on to consumers in the prices of goods and services.

Many segments of the population would favour a legislative approach. The 1992 Canadian Privacy Survey found that a clear majority of Canadians favoured government legislation or a government/private sector partnership to develop privacy protection guidelines for the private sector. A 1992 Equifax Canada study of Consumers and Privacy in the Information Age found that 84 percent of the insurance, financial and credit bureau executives surveyed believed that federal legislation is required to set rules for the collection and circulation of consumer information, thereby avoiding a patchwork of disparate provincial regimes. While this appears to go against today's trend toward a deregulatory environment and reduction of government, it may in fact recognize that harmonized basic rules

for data protection are good for business and may be possible without excessive bureaucracy. Setting ground rules enables all players to compete fairly, and establishes consumer confidence.

## **Voluntary Codes and Standards**

Voluntary codes have been the preferred approach of Canadian business and industry associations. This approach allows for flexibility in application, so that different industries can tailor their data protection schemes to the needs of their customers, the regulatory environment in which they operate and the demands of the marketplace.

There is no need for voluntary codes to be any less stringent than those enforced by law, but it is this very matter of enforceability that is giving consumer advocates grounds for concern. Who is ultimately accountable? To whom does an aggrieved consumer go for redress? As the value of personal information increases with the growth of the information economy, how can voluntary codes unsanctioned by law ensure its protection? Past experience with voluntary codes has not been encouraging because they frequently do not meet the 1981 OECD Guidelines. As a result, they are considered by most privacy experts as inadequate to cope with the privacy threats of the 1990s.

The CSA's project to develop a national privacy standard extends the voluntary code approach. By setting out the basic principles that must be addressed in a code, the standard strengthens the often weak and ambiguous language used in codes. Oversight in the form of auditing and certification by a standards



body, such as the Quality Management Institute, a division of the CSA, could provide a level of protection similar to that in a legislated regime. Successful privacy protection by means of the proposed CSA voluntary standard, however, will be difficult if it is not adopted fully and implemented broadly by industry associations and companies.

Contractual approaches also have been suggested, whereby consumers would agree to the use of their data for specific purposes, perhaps in return for discounts or fees. Care must be taken that such a market-driven approach does not result in privacy for only the rich. At present, few individuals understand the market value of their personal information or know how to protect it. In addition, contracts that limit or waive fundamental privacy values have the potential to become an industry practice in the absence of clearly defined privacy rights.

### ***Technological Solutions***

Another approach to privacy protection is to use technology to safeguard personal data. Traditionally, technology has been exploited to increase the amount of information gathered, and hence has been feared rather than welcomed by privacy activists. But technology itself is neutral, and can be used to enhance privacy as well as threaten it. Technologies can be designed so that the "default setting" is on zero information collection. Telephone systems can be designed to "forget" the last few digits of a telephone number after placing a call, in order to protect privacy in personal billing statements. Electronic mail

systems can be developed that provide ephemeral messages for personal use, a sort of electronic disappearing ink. Should the design for the information highway explicitly enhance the ability of the individual to control his or her personal and transactional information?

An important yet underexplored territory is encryption or encoding. Strong encryption is now available and can be incorporated into software, embedded as chips in equipment such as telephone sets or palm-sized computers, or used in smart cards. Smart cards, through the use of public key encryption, can provide fraud-proof guarantees of identity or credentials, and yet allow the holder to be completely anonymous. The same technology can be used to provide reliable but virtually untraceable electronic cash — a far safer method for the consumer than releasing a charge card number over the information highway.

Technologies brought to market can have profound effects on the rights of consumers, but how can consumers affect the technology development process? Should there be public hearings, such as the CRTC has for telecommunications services when a new technology is brought to market? Should the privacy implications of all new information systems and standards be explored in public fora? Is it a responsibility of government, or should it be up to the marketplace to determine what levels of privacy protection will be offered? Should privacy be an optional extra, for which only some Canadians can afford to pay, or should privacy be cost-neutral and considered an essential part of service offerings?

### ***Consumer Education***

There is a fundamental need to educate businesses about the need for more enlightened approaches to the handling of personal data, and to raise the awareness of consumers about how to protect themselves. Consumers need information and education about their rights, about the value of their personal information, about the risks to their privacy that new technologies can bring, and about what they can do to retain privacy. Although most Canadians see the role of protecting privacy as a government responsibility or perhaps a partnership of government and business, they also feel that the individual has a strong role to play in solving privacy problems. What should be the relative balance of responsibilities?



# 6

## Public Comment

The intent of this paper is to contribute to the debate on the social and economic impact of the information highway, not to offer definitive solutions. Comments from individuals, organizations and institutions in both the private and public sectors are welcome. Written submissions and/or comments on the approaches to privacy protection are invited on the following questions, or on any portion of this discussion paper. They should be sent to the address mentioned in the Preface.

- What principles should form the basis of effective privacy protection?
- Does government need to introduce stronger measures to protect the privacy and security of information? How can each of the four approaches described above be used effectively?
- Is a national level of privacy protection needed, or can adequate privacy protection on the information highway be provided through provincial or sectoral legislation?
- In which circumstances might voluntary privacy guidelines developed by businesses be appropriate?
- Should the information highway be designed to provide high levels of privacy protection, or will this slow the pace and raise the cost of innovation?
- How can Canadians become better involved in the design process for potentially privacy-threatening technologies and services?
- How can Canadians become better informed about the value of their personal information and the need for controlling its use? What role should businesses and governments play in educating the public?

# Annexes

## **A — Chronology of Background Events**

The issue of privacy in an information-based economy arose globally in the 1970s. In Canada, the former Department of Communications joined with the Department of Justice in forming the Task Force on Privacy and Computers, which issued a report titled *Privacy and Computers* (Ottawa: Information Canada, 1972) and several studies. At the OECD, privacy was addressed as an issue of transborder data flows. Member countries realized that they had a common interest in protecting privacy and individual liberties, and in reconciling the fundamental but competing values of privacy and the free flow of information. It was recognized that transborder flows of personal data contribute to economic and social development, and that restrictions on these flows could interfere with the operations of multinational enterprises and cause serious disruptions in important economic sectors such as banking, insurance and travel. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were promulgated. At about the same time, the Council of Europe passed a similar document, Convention 108, to which European countries varied greatly in their legislative responses. It was the sluggishness on the part of member states to take action that prompted the European Community to introduce much stiffer Community directives with the force of law.

Key events and players are listed below in chronological order:

- 1969 OECD recognizes privacy implications of transborder data flow; Group of Experts struck in 1978
- 1970 U.S. *Fair Credit Reporting Act*
- 1972 Report of the joint Justice–Communications task force on privacy and computers
- 1977 Privacy Commissioner established under *Canadian Human Rights Act*
- 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- 1981 Interdepartmental Task Force on Transborder Data Flows struck in Canada
- 1982 Council of Europe passes Convention 108 on data protection; Canada passes *Privacy Act* for federally held records
- 1984 Canada signs OECD Guidelines; Department of Justice responsible for urging compliance of industry
- 1987 Report of Standing Committee on Justice reviewing *Privacy Act* implementation criticizes lack of compliance with OECD Guidelines in private sector and government inertia



- 1990 European Community tables draft directives on data protection and data protection in telecommunications; U.S. and international players mount vigorous lobby to water down transborder data flows and trade-restrictive aspects of directive
- 1991 OECD revisits data protection; European Community seeks to protect its privacy directives in the General Agreement on Tariffs and Trade; key federal departments back CSA's bid to develop a model OECD-based code of practice, along with industry and consumer groups
- 1992 Department of Communications tables Telecommunications Privacy Principles and drafts legislation on cellular privacy
- 1993 Federal government passes new *Telecommunications Act*, which came into effect October 25, 1993, giving CRTC a specific mandate with respect to the protection of privacy in telecommunications and substantial powers to exercise this mandate; Quebec passes Bill 68, law on protection of personal information in the private sector, which came into effect January 1, 1994

## ***B — The OECD Guidelines and the Draft CSA Privacy Standard***

Drafted at the end of the 1970s and adopted as a recommendation of the Council of the OECD in September 1980, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data provided a sound basis for fair information practices at the time, and constituted a remarkable document for a group of countries largely without data protection laws. Nevertheless, the Guidelines may require some further specifications in the context of the technologies of the 21st century. The main concepts are as follows:

- Eight basic principles of national application are set out in Part Two of the Guidelines, covering data Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation and Accountability.
- Four principles of international application covering Free Flow and Legitimate Restrictions are set out in Part Three of the Guidelines.

When the CSA went about drafting its model privacy code, it used the OECD Guidelines as a starting point, interpreting them afresh in the Canadian context of 1991. It is important to evaluate the CSA standard in its entirety, since the commentary on the principles is important to the understanding of each principle. However, because the draft is not yet available for public discussion, its 10 principles are listed below only briefly, with a note where there is deviation from the OECD Guidelines. Public comment on the final draft will be invited in the fall of 1994.

1. Accountability (seen to be so fundamental that it must be the first principle)
2. Identifying purposes
3. Consent (new)
4. Limiting collection
5. Limiting use, disclosure, retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance (new; gives individual the right to challenge an organization's compliance with any of the principles, not just the accuracy of the individual's data)

## **C — Telecommunications Privacy Principles**

- Canadians value their privacy. Personal privacy considerations must be addressed explicitly in the provision, use and regulation of telecommunications services.
- Canadians need to know the implications of the use of telecommunications services for their personal privacy. All providers of telecommunications services and government have a responsibility to communicate this information in an understandable and accessible form.
- When telecommunications services that compromise personal privacy are introduced, appropriate measures must be taken to maintain the consumers' privacy at no extra cost unless there are compelling reasons for not doing so.
- It is fundamental to privacy that there be limits to the collection, use and disclosure of personal information obtained by service providers and generated by telecommunications networks. Except where clearly in the public interest, or as authorized by law, such information should be collected, used and disclosed only with the express and informed consent of the persons involved.
- Fundamental to privacy is the right to be left alone. A balance should exist between the legitimate use of unsolicited telecommunications and their potential for intrusion into personal privacy. All parties have a responsibility to establish ground rules and methods of redress so that Canadians are able to protect themselves from unwanted and intrusive telecommunications.
- Privacy expectations of Canadians may change over time. Methods of protecting telecommunications privacy must be reviewed from time to time to meet these changing expectations and to respond to changing technologies and services.