PRIVACY AND THE CANADIAN INFORMATION HIGHWAY

REVIEW OF COMMENTS RECEIVED ON THE INDUSTRY CANADA DISCUSSION PAPER

AKAY INFORMATION CONSULTING INC.
P.O. BOX 1268, CARLETON PLACE
ONTARIO, K7C 4L4
(613) 257-1072

March 1995

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

The seventy-six responses received cover a wide spectrum of interests and expertise. In order to simplify comparisons between them, the responses have been broken down into eight categories. These categories and the relevant number of responses in each are as follows: Medical and Social Research (21); Telecommunications and Technology (12); Individuals (11); Consumer and Privacy Advocates (11); Financial Services, Credit and Marketing Groups (5); Privacy Commissioners (4); Government (4); Miscellaneous (8).

Each of the submissions is summarized in regard to general comments on privacy, privacy concerns and various methods of ensuring privacy. Specific proposals and recommendations, stemming from the four main potential approaches set out in the Discussion Paper, are included in each summary, where applicable. These various elements are brought together and summarized in the review itself, which includes conclusions resulting therefrom.

WHAT IS PRIVACY?

The definition of privacy set out in the Discussion Paper is generally accepted by the great majority of respondents.

One of the questions that frequently comes up is "Who owns personal information?". The majority of consumer and privacy advocates and privacy commissioners believe that personal information is owned by the individual. However, most private sector organizations tend to see it as a commodity over which the consumer has varying degrees of control.

A number of respondents contend that the right to privacy should be incorporated in the Charter of Rights and Freedoms. However, recognizing the difficulty of amending the Charter, they are of the opinion that any amendment to the Privacy Act or any new federal privacy legislation should include a preamble that recognizes the principle of privacy.

WHAT ARE THE PRIVACY CONCERNS?

The great majority of respondents, including those from the private sector, acknowledge that there is strong and growing public concern about privacy protection on the information highway. This view is corroborated by a number of privacy surveys that have been conducted over the past few years. The most quoted of these surveys are the Ekos survey of 1992, the Equifax survey of 1992 and the poll done by Gallup Canada in 1994.

There is considerable concern about freedom from intrusion. Monitoring and surveillance are seen to be the most potentially damaging forms of intrusion. Typical examples include, tracking the whereabouts of an individual by wireless or satellite-based personal communications systems, tracing the market profile of an individual from the "data shadow" cast by a series of transactions, and employee surveillance. Surveillance of E-mail, including the related question of who owns the E-mail message, also is seen as a problem. Monitoring of cellular phone messages by the use of scanners, as well as electronic surveillance in the home, also rate highly. Nevertheless surveillance and monitoring are seen to have some benefits, particularly in the fields of search and rescue, home security and fleet management. It all depends on the uses to which they are put. Lesser forms of intrusion are seen as being more of an annoyance, such as telemarketing which the individual can terminate at will.

The protection of personal information is the major concern of the public. This is expressed by the lack of control that an individual has over his/her personal information. The use of personal information to create personal profiles of individuals, as well as a perceived lack of security and protection for personal information holdings, also are significant issues. The unauthorized use of the Social Insurance Number (SIN), protection of medical and health information, and cross-border transfers of information are also of great concern to some respondents. Equally, business is concerned that the social and economic benefits of the collection and use of personal information must be recognized. Some journalists and writers fear that the freedom of expression provisions of the Charter could be subverted by unwarranted privacy rules. Mention is also made of the strange ambivalence that occurs within the general public. Very often members of the public believe that it is their right to know all the sordid details of the personal lives of celebrities but would be horrified if the same information was divulged about themselves.

The continuing and rapid evolution of technology raises a concern that privacy could become the victim of creeping erosion. Security of stored data is also a significant concern. Nonetheless, there is a growing acceptance of the use of technology, coupled with the benefits it can bring. On the other hand, business is concerned that privacy requirements not be allowed to inhibit the introduction of new technologies. A fair balance is required between the demands of technology development and privacy protection.

Some of the foregoing concerns can be attributed to a feeling of lack of knowledge and power on the part of individuals. In particular, they often do not know just who holds information about themselves and they feel vulnerable in the light of well-publicized privacy infractions.

Medical and social research, as it relates to the protection of personal information, is a significant issue. By far the greatest number of responses

come from medical and social researchers. They are concerned that strict privacy rules could prohibit the long term storage of personal medical and health data and could mandate prior consent for the use of such data, in spite of the very high levels of security provided. If this occurs, much valuable medical and social research, which is directed toward the public good, could be stifled. Examples include, tracking the incidence of fatal diseases such as cancer and heart disease and undertaking studies as the basis for important government decisions in the social policy field.

In overall terms, there is a strong belief, expressed by many respondents from all sectors, that if the various concerns of the general public are not alleviated, the information highway will not be used to its full potential.

HOW TO ENSURE PRIVACY

As a background to potential changes in privacy protection, some respondents provided details of the historical evolution of the development of privacy practices and legislation both in Canada and abroad. It is noted that in Canada, only the federal government and five provinces have legislation to protect personal information held by governments. Only Quebec has legislation governing the protection of personal information in the private sector. At the federal level, some sector specific legislation, governing such areas as telecommunications and financial institutions, makes provisions for the implementation of regulations in regard to the management of personal information. To date, however, regulations have only been implemented in the telecommunications sector. The development of voluntary privacy codes in the private sector also is traced. In the overall scheme of things, these scattered developments are seen as an unsatisfactory patchwork approach. They are confusing and difficult to understand by the average individual and will not address emerging international standards, the dangers of rapidly evolving technologies, or the expectations of the public.

International developments are also reviewed. Europe is seen to lead the world, particularly over the last 10 to 15 years. Commencing in 1982, the Organization for Economic Cooperation and Development (OECD) published a set of privacy guidelines. The guidelines contained comprehensive personal data protection principles, coupled with provisions for the restriction of transborder flows of personal data to countries which did not have equivalent protection standards. Relatively all privacy legislation in Canada is based on the principles found in the OECD guidelines. At the present time, the guidelines are being updated into directives by the European Communities (EC) and compliance will be mandatory for all members, once they have been passed by the European Parliament. The most important factor about the proposed directives, from Canada's viewpoint, is that they have the potential to inhibit trade by preventing the flow of personal information, whether in automated or manual

form, to countries that do not have adequate data standards. At the present time, it is doubtful that Canada would qualify because it does not have national standards governing the private sector. Privacy developments in the USA also are summarized. The USA does not have national standards applicable to the whole of the private sector, nor does it have legislation covering the public sector which meets all of the provisions of the federal Privacy Act.

The Discussion Paper's call for input on principles that should form the basis of effective privacy protection met with a wide range of responses. Most of this input was based on the OECD guidelines. Basic to the arguments of some consumer and privacy advocates and privacy commissioners is the premise that the right to privacy is a basic human right. Stemming from this, is the view that the right to control one's personal information is the most important factor, coupled with the principle of consent. However, some variations of viewpoint exist in regard to the question of consent. Many consumer and privacy advocates and privacy commissioners see consent as meaning "informed consent". However, in the private sector consent tends to be seen as "consent", no matter how obtained. Moreover, consumer and privacy advocates and privacy commissioners tended to see consent as "opting-in", whereas the private sector sees it as "opting-out". One of the additional principles raised, beyond those contained in the OECD guidelines, is the principle that individuals should not have to pay to maintain basic and existing levels of privacy. Again, there are differences of viewpoint on this issue. Some respondents believe that levels of privacy above the basic level should be paid for, while others maintain that privacy should not be prejudiced by inability to pay. Another principle entails freedom of individuals to choose whether or not to connect to the information infrastructure, to accept or reject services that may affect their level of privacy, and to be free to sub scribe to, and be charged for, only those services they wish to receive. However, they should not suffer reduced levels of service because of their choice. Nevertheless, in overall terms, there is little difference in views. Most respondents support the principles contained in the Canadian Standards Association's (CSA) draft "Model Code for the Protection of Personal Information". Other submissions propose principles that should govern the information highway itself.

An emerging problem is seen in the blurring of distinction between information which is resident in the public sector and that which is resident in the private sector. In Europe, this distinction between the public and private sectors, in terms of privacy protection, has been rendered irrelevant by the proposed EC directives. Within the private sector, a further blurring is evident. With the increasing integration of various media on the information highway, the original distinction between the various players, e.g., telephone and cable companies, the press, broadcasters, and marketers, it is becoming increasingly difficult to establish clear boundaries

between sectors. Accordingly, the effective establishment of sectoral voluntary codes could become more problematic.

The patchwork system of federal/provincial legislation and private sector voluntary codes across Canada is stimulating the call for a "level playing field". Different legislation in different jurisdictions results in "rich and poor" in terms of privacy protection. Some provinces have no legislation at all, while Quebec has legislation covering both the public and private sectors. This could lead to the establishment of "data havens" where companies can locate to avoid privacy protection requirements, thus leading to unfair competition. Therefore, all players are interested in the establishment of a national privacy standard. However, how this is to be done results in different opinions.

The main focus of the Discussion Paper centered around approaches to be used in promoting privacy protection in the private sector. Four potential approaches were identified, legislation and regulation, voluntary codes and standards, technological solutions, and education. While there is very little difference in views on the roles to played by the two latter approaches, there is considerable debate on the relative merits of legislation and voluntary codes.

The majority of respondents believe that the government needs to take stronger action and establish new legislation. With only two private sector respondents being in favour of legislation, the majority of support for this approach comes from consumer and privacy advocates, privacy commissioners and individuals. The benefits of legislation and regulation are seen as guaranteeing to all Canadians an equal level of privacy protection and providing a legal means of redress, sanctions, complaint and appeal. In addition, such a regime would meet the standards of the EC, thus avoiding potential trade problems. Many suggestions are made as to how this may be accomplished. The preferred method is for legislation to establish a framework for a set of national privacy standards under which private sector codes would operate and be bound. This could be complemented by an independent and impartial administrative body which would enforce compliance, hear complaints, provide redress and deliver sanctions. Suggestions are made that such a system could be based on the Quebec Act. Moreover, lack of bureaucracy, low costs and cost effectiveness are seen as prerequisites. A phase-in period is recommended, together with early consultations with the provinces to harmonize both public and private sector legislation across the country. Other suggestions include amending and updating the federal Privacy Act to bring it into line with the proposed legislation and for the public sector to "clean up its own shop". In effect, it is contended that the federal government must assume a strong leadership role. Meanwhile, opponents of the legislative route point its problems. It is seen as inflexible, incapable of rapid change to accommodate the rapidly evolving technology and marketplace, and possibly inhibiting new initiatives and investment. The

time taken to reach a federal/provincial consensus is seen as a problem, as is the fact that it would go against the current trend of deregulation in the global marketplace. Moreover, it would cost more in a period of fiscal restraint. The private sector is generally against legislation. The telecommunications industry, in particular, is against additional legislation for the protection of personal information because it believes that privacy directives issued by the Canadian Radio-Television and Telecommunications Commission (CRTC) are sufficient to meet privacy concerns. On the other hand, it is strongly in favour of technology-specific legislation that would make it an offence to intercept radio-based telecommunications and which would generally prohibit the manufacture, importation, sale and distribution of scanners capable of monitoring radio-based telephones, including cellular phones. Nevertheless, the private sector is not universally against general privacy legislation, provided that it is implemented only after voluntary codes have been given a chance to prove themselves and have been shown not to work. Additional provincial legislation, in the absence of federal legislation, is not seen as viable because it would not lead to uniform standards across Canada.

Voluntary codes and standards are mostly favoured by the private sector because of their flexibility and adaptability in meeting the particular needs of different technologies and segments of the marketplace. They are also seen as less costly to operate, can raise the profile of privacy within an organization, and can help to educate consumers. Moreover, they can be national in scope and provide a level playing field within each sector. In addition, they are capable of being made mandatory across all members of a sectoral organization or can be strengthened by peer pressure, compelling competitive interests and consumer demand. The main objection to voluntary codes and standards is that they are just that, "voluntary". Many are not seen as fully responsive to consumer concerns, in that they do not meet the full range of fair information practices and do not have adequate mechanisms for complaint and redress. Also, they are sometimes tailored more to business interests than to consumers' privacy rights. Moreover, they may not meet the "adequate" standards of privacy protection required by the proposed EC directives. This being said, consumer and privacy advocates and privacy commissioners are not completely against voluntary codes. They are considered to have an important role to play, because of their flexibility and adaptability, provided they are governed by overarching legislation. In this regard, both the private sector and the consumer and privacy advocacy and privacy commissioner groups strongly support the recent initiatives of the CSA to develop a voluntary privacy code as a national standard. The CSA draft code is being developed by a working committee comprised of representatives of governments, privacy commissioners, consumer and privacy advocates and the private sector. The code, when implemented, could provide a standard against which private sector voluntary codes could be measured and may meet the adequacy provisions of the EC privacy directives.

Technological solutions are also seen as having a part to play. Technology can threaten privacy but new developments can now allow privacy protection features to be built in at the outset. In this regard, a number of respondents see the need for privacy impact assessments to be made an essential part of the systems development process. Whether the information highway should be designed to provide high levels of privacy protection and whether it will slow the pace and raise the cost of innovation is also addressed by many respondents. Built in security measures are seen as a key in this regard. New innovations in this area include advanced encryption, the use of smart cards and the implementation of digital technology. Basic protective measures are seen as essential, coupled with additional measures which could be provided at extra cost. Furthermore, it is suggested that the government encourage the development of new protective technologies and provide support for research and development in order to provide new opportunities for Canadian industry. In general, privacy protection measures are not seen as increasing the cost of innovation, provided they are not too excessive. There is a wide variety views on how Canadians can become better involved in the design of potentially privacy-threatening technologies. Avenues already exist, such as involvement in CRTC hearings and participation in the development of new CSA technical standards. However, many in all sectors see the need for more direct involvement at the design stage, provided that it is limited to informal consultations and the provision of advice by such groups as consumer advocates and privacy commissioners.

Lack of awareness and confusion on the part of the public are seen as significant problems. Therefore, there is wide agreement that consumer education is essential. Education of employees and businesses on their privacy responsibilities also is seen as necessary. There is a general consensus that both governments and business have a major responsibility in this area. Most businesses indicate commitment and many are already engaged in education programs. As well, consumer and privacy advocates and privacy commissioners indicate willingness to become involved, provided that funding and resources are made available. However, it is also recognized that consumers themselves have responsibilities and must also take initiatives in this area. The educational tools available are seen to be many and varied. These range across the publicizing of private sector privacy codes and the CSA code, periodic public awareness campaigns, production of material and brochures aimed at different elements of the public for distribution in information centres and libraries, etc.

CONCLUSIONS

There is a wide range of real public concerns on privacy matters which, if not addressed quickly, could escalate to the point that the effective functioning of the information highway could be jeopardized.

There is a significant divergence of views between the majority of members of the private sector and consumer and privacy advocacy and privacy commissioner groups on the relative merits of legislation and voluntary codes. However, there also is a pragmatic and conciliatory approach to these differences which makes a compromise achievable.

No single approach to the resolution of the problems is viable. Therefore, a combination of the approaches outlined in the Discussion Paper is most likely to succeed because they are inter-related and mutually supportive.

In order to achieve comprehensive solutions to the various problems identified by respondents, within the minimum possible time frame, a well-coordinated plan should be developed.

The following are potential elements of a plan which the Advisory Council may wish to consider.

- The establishment by legislation of a national framework of privacy standards, probably based on the CSA model privacy code, under which private sector codes would operate and be bound.

- Revisions to the federal Privacy Act to overcome its current shortcomings, including a revised preamble, provision for the protection and security of personal information, and provision for the establishment of privacy impact assessments within the public sector.

- Development of a program to reinforce, strengthen and update the application of privacy protection practices within the public sector.

- Early discussion with the provinces to implement national standards on a country-wide basis.

- Development of legislation to make it an offence to intercept private radio-based telecommunications, and to generally prohibit the manufacture, importation, sale and distribution of scanners capable of monitoring radio-based telephones, including cellular phones.

- Development of a program to systematically promote the development of private sector codes based on the CSA model privacy code.

- Creation of a joint government/industry program to promote and support the development of privacy protection technologies.

- Promotion of consultations between industry/government, consumer groups and privacy commissioners on the development of significant and new potentially privacy-threatening technologies and systems.

- Development of a joint industry/government privacy education program in consultation with consumer groups and privacy commissioners.

- Establishment of consultations between government and the medical and social research groups to resolve the apparent dichotomy between the protection of personal information and the need to carry out medical and social research necessary to promote the public good.

- Development by the govemment of a standard privacy protection clause for all contracts or agreements involving the transfer or exchange of personal information with all institutions outside of government.

- Issuance of a public announcement after adoption of the plan and ministerial approval.

Failure to address the major problems identified by respondents could be followed by increasing public privacy concerns, coupled with avoidance of use of the information highway. Also, it might lead to Canada's privacy protection standards being considered inadequate under the EC privacy directives.

INTRODUCTION

Origin of the Discussion Paper

In October 1994, Industry Canada, in cooperation with the Information Highway Advisory Council, issued the discussion paper "Privacy and the Canadian Information Highway". The paper was the first of several discussion documents to be released by Industry Canada on social, economic and technology policy issues. Its purpose was to seek the public's views and to raise the level of debate on privacy issues related to the development and operation of the information highway. Written submissions and/or comments were invited on its contents, including the various options and approaches set out in the paper. Submissions were to be received by December 23, 1993. Copies of the individual submissions are available for viewing, for a period of one year, at the Industry Canada Library, 2nd Floor, Journal Tower South, 365 Laurier Avenue West, Ottawa, Ontario, and at the regional offices of Industry Canada in Halifax, Montreal, Toronto, Edmonton and Vancouver.

Responses Received

The seventy-six responses received cover a wide spectrum of interests and expertise, and range in size from one page to sixty pages. In order to simplify comparisons between them, the responses have been broken down into eight categories to reflect the main affiliation of the respondents. These categories and the relevant number of responses in each are as follows: Medical and Social Research (21); Telecommunications and Technology(12); Individuals (11); Privacy and Consumer Advocates (11); Financial Services, Credit and Marketing Groups (5); Privacy Commissioners (4); Government (4); Miscellaneous (8). The Miscellaneous category is comprised of a labour organization, a standards organization, a telecommunications security company, a journalist, a writer/TV producer, an expert on learning and training, and two international respondents. Summaries of the actual submissions, by category, are contained in Appendix A.

Basis of Review

Each of the submissions is summarized in regard to general comments on privacy, privacy concerns and various methods of ensuring privacy. Specific proposals and recommendations, stemming from the four main potential approaches set out in the Discussion Paper, are included in each summary, where applicable. These various elements are brought together and summarized in the review itself, which includes conclusions resulting therefrom.

WHAT IS PRIVACY?

Definition

The right to privacy is defined in the Discussion Paper as comprising two elements:

> the right to be left alone, free from intrusion and interruption; and,
>
> the right to exercise control over one's personal information.

Both explicitly and by reference to examples, this definition is accepted by most respondents. However in two cases, amendments to the definition are proposed.

In the first case, use of the word "interruption" is questioned by one of the technology associations as adding nothing to the concept of privacy because its use suggests that all interruptions - whether welcomed or not - are invasions of one's privacy. Therefore, it submits that the concept of "uninvited" is the key to any notion of privacy intrusion in today's society.

The second comment comes from one of the consumer and privacy advocates. In its view, the concept of privacy should be expanded to include the concept of "reputation" (as recognized by the Quebec Charter), in as much as personal information can shape what one thinks of someone. Furthermore, it should also be expanded to include the concept of "dignity" (also recognized by the Quebec Charter), as it relates to one's "informational identity".

Who owns personal information?

The question of who owns personal information is seen as elemental to privacy rights by some privacy and consumer advocates as well as by the Privacy Commissioner. Their belief that personal information is owned by the individual is perceived as a fundamental premise underlying control over its collection, use, disclosure, retention and disposal.

Contrary to this view, most of the private sector organizations seem to be more of the view that personal information is a commodity over which the consumer should be able to effect varying degrees of control. However, one technology association likens discussion about the ownership of transactional information as being similar to discussion about intellectual property.

Privacy - A Charter Right?

A number of respondents, particularly privacy and consumer advocates, believe that the right to privacy should be incorporated in the Charter of Rights and Freedoms. The basis for this view is that privacy is a fundamental human right that must be recognized.

However, recognizing the difficulty of amending the Charter, an alternative proposal is that any amendment to the Privacy Act or any new federal privacy legislation should include a preamble that recognizes the principle of privacy. This would be commensurate with a similar provision in the proposed privacy legislation of the European Communities.

WHAT ARE THE PRIVACY CONCERNS?

Are there real privacy concerns?

Confirming the generally accepted view, the vast majority of responses specifically point to a large and growing consumer concern over privacy matters, particularly in regard to the information highway. There is little difference in views in this regard, whether they come from the private business sector, consumer and privacy advocates, privacy commissioners or individuals at large. These concerns are shown to be evidenced by privacy surveys over the last few years and a number of these surveys are specifically quoted.

The Ekos survey "Privacy Revealed - the Canadian Privacy Survey" was conducted on behalf of a number of private and public sector organizations in 1992 and is the most oft quoted in the responses. It showed that while 52 percent of Canadians are extremely concerned about privacy, 92 percent expressed at least moderate concern. Moreover, 83 percent strongly believe that they should be asked for their permission before an organization can pass on information about them to another organization, and 71 percent totally agree that privacy rules should apply to both government and business. Also, "there is a pervasive sense that personal privacy is under siege from a range of technological, commercial and social threats". Furthermore, greater concern was expressed about business sector organizations than about public sector organizations. However, as pointed out by some business sector members, the survey also revealed that privacy is of more concern in the abstract. Thus, while Canadians are concerned about controlling their personal information, they are more accepting of its use in specific situations where the purposes and benefits are clearly identified.

The 1992 "Equifax Canada Report on Consumers and Privacy in the Information Age" also found that a strong majority of consumers are worried about threats to their privacy. However, an equally strong majority agree that computers give people more convenient access to useful information and services and have improved the quality of life. Moreover, the same majorities responded positively to the use of personal information in setting automobile rates, in approving loans, and in issuing a credit card or establishing credit limits. The report concluded that 62 percent of "Canadians take a pragmatic approach to balancing privacy interests and access to valued consumer benefits, deciding area by area what kind of fair information practices, rules and protection are called for, and who should apply them".

In 1994, a poll done by Gallup Canada for Andersen Consulting on "What Canadians Think About the Information Highway" indicated that, while 67 percent of Canadians thought that the information highway was a good

idea, 83 percent were very or somewhat concerned about how the highway might affect their privacy. However, contrary to the views expressed in this survey, a 1993 Decima Research survey found that 70 percent of respondents thought that society is relying too much on technology and 61 percent thought that technology makes things more complicated instead of simpler. In the 1994 TELUS Longwoods survey 39 percent of respondents felt that they would be so concerned about privacy invasions that they probably would not use the information highway.

These findings are reinforced and renewed by the fact that almost all of the comments received from individuals related to concerns about the protection of personal information and freedom from intrusion.

The extent of concerns is very broad, ranging across freedom from intrusion, protection of personal information, lack of knowledge and power, and technology.

Concerns re Freedom from Intrusion

These concerns are related to the right to be left alone. Although the Discussion Paper lays great emphasis on a discussion of the four approaches which might alleviate privacy concerns related to the protection of personal information, considerable concern is also expressed by respondents on the issue of uninvited intrusion. These concerns are equally expressed by both the business sector and the consumer sector, and may be divided into two broad areas. The first area involves monitoring and surveillance and the second involves unwanted or annoying intrusions into a person's time.

Monitoring and surveillance is seen to be by far the most annoying and potentially damaging intrusion and many examples are given. A typical example is the "electronic leash" created by the enhanced tracking capabilities inherent in wireless or satellite-based personal communications systems whereby, in the absence of effective controls, the actual location and movements of an individual can be tracked in an unauthorized manner. Also, the "data shadow" cast by an individual in a series of transactions on the information highway, can be assembled into a pattern which will allow a profile to be developed of an individual's lifestyle, personal habits, and buying power and preferences. Employee monitoring, whether by video surveillance or electronic productivity monitoring, is also seen as a significant issue. Surveillance of E-mail, whether by employers or outside sources, is both a concern and, in regard to employer monitoring, has caused an active debate as to whether the employer has the right to monitor personal messages sent by E-mail. A most vociferous concern re surveillance and monitoring relates to the use of scanners to intercept cellular or other radio-based private communications. This concern is expressed both by the consumer sector and the telecommunications sector,

as is the recent issue over call blocking of name display telephone services. Finally, surveillance at home is also seen as a potential problem in the light of proposed systems which will allow the provision of security services by electronic means, electronic monitoring of consumption and service by utility companies, and interactive multimedia services on TV and home computer systems. Nevertheless, surveillance and monitoring are not seen as totally negative. Their significant benefits are recognized in the fields of home security, search and rescue, commercial fleet management, etc. It is all a question of the uses to which monitoring and surveillance are put.

Unwanted or uninvited intrusions into a person's time are also seen as a concern but, as evidenced by responses to polls and from respondents, not to the same degree as monitoring and surveillance. While the former is seen as an annoyance, the latter is seen as potentiality threatening. However, telemarketing is deemed to be more of an intrusion than ad-mail, although the recent CRTC decision banning the use of automatic dialing-announcing devices (ADADs) for commercial solicitation and restricting the hours during which "live" telemarketing can occur should do much to alleviate the problem. In any event, the consumer usually has the ability to terminate the intrusion at will.

Concerns re Protection of Personal Information

A perceived inability to control access to and the use by others of an individual's personal information is seen as the major privacy concern. Allied to this is the unauthorized marketing of personal information. These concerns are equally recognized by business organizations, consumer and privacy advocates and privacy commissioners. It is also the concern most frequently expressed by individuals.

The unauthorized use of transactional data and the compilation of personal profiles by the matching and linking of personal information are significant issues. Whether they take place as a result of involvement in credit card, direct marketing or banking transactions, etc., or as a result of obtaining medical services, all are seen as being major areas of concern.

Lack of adequate security and protective measures is also worrisome. This can be due to lack of knowledge or laxity on the part of employees of the organization holding the personal information or to lack of built-in or established security/protective measures.

A number of specific issues related to particular types of personal information are also evident. Of these, use of the Social Insurance Number (SIN) and the protection of medical and health information are the most important. Lack of control on the use of the SIN by both the private sector and by those elements of the public sector which do not have specific authorization for its use are seen as a concern in a number of responses

from individuals. Also, the protection of medical and health information related to individuals is seen as particularly sensitive. Concerns in this latter regard come not only from individuals, consumer and privacy advocates and privacy commissioners but also from the private sector and the medical research community.

Another area of general concern is the issue of cross-border transfers of personal information. Here, the worry is that personal information will no longer be subject to national or provincial jurisdiction and therefore may not be capable of being protected.

Seemingly contrary to these concerns, is the concern that the business, economic and social benefits of the collection and use of personal information must be recognized. Business benefits are expressed in terms of the extension of markets and the ability to provide new and better services. Economic benefits are seen as the ability to provide additional employment in such areas as the direct marketing industry, while social benefits are seen to include law enforcement, medical and social research as well as the ability to implement consumers transactions in a more effective, efficient and less costly manner. Not only is this concern expressed by the business community and medical and social researchers, but the benefits also are recognized by consumer and privacy advocates as well as privacy commissioners.

Two journalist/writers express fears that privacy initiatives could restrict access to large numbers of records, even though anonymized. This could prejudice the freedom of expression provisions of the Charter of Rights and Freedoms. Some private sector organizations are concerned that network providers may be seen as the information highway's privacy police. In this regard, a number of respondents agree that this would be an impossible task and that privacy measures should focus on the information providers who interact on the highway. Also, there is concern that it should be recognized that consumers also have a responsibility in the protection of their own privacy.

On the matter of privacy in general, a few respondents have noted the strange ambivalence that occurs within the general public. While supporting the need for the adoption of strong privacy principles, particularly when they themselves are directly affected, many are not so concerned when their fellow citizens are affected. This is expressed in the call for information about the whereabouts of convicted criminals who have served their sentences, e.g. rapists and child molesters, the hunger for details of the personal lives of public figures as published in the tabloids, and the support for using new technologies to root out fraud and abuse, eliminate waste and duplication, and streamline inefficient bureaucratic procedures.

Concerns re Technology

The continuing and rapid evolution of technology, coupled with the benefits it can bring, raise a concern that privacy could become the victim of creeping erosion. It is not so much the actual applications of technology that cause the greatest concern but the fact that privacy may be left behind or overlooked in the "onslaught of technology". Coupled with this, is the equal concern that privacy safeguards are too often not "built-in" to the development of technology but are "bolted-on" as a later and perhaps ineffective appendage.

In spite of these concerns, it is acknowledged that there is a growing public acceptance of the use of technology. This is illustrated by the use of automated banking machines (ABMs), the Interac direct payment service, personal computers, modems, the Internet, electronic tax filing, etc.

However, a contrary concern, particularly on the side of the business sector, is that privacy concerns or requirements may inhibit the development of new and innovative technologies. Therefore, they see a fair balance as being required between the demands of technology development and privacy protection requirements.

Concerns Based on Lack of Knowledge and Power

Some of the foregoing concerns can be partially attributed to a perceived lack of knowledge and power on the part of consumers. Individuals become frustrated because they are not aware of exactly what technology can do and therefore may have little understanding of the privacy implications that may be involved. Equally, they feel powerless in many circumstances, particularly because they do not see any effective means of redress for privacy related complaints against the private sector.

Specific concerns in this area relate to the fact that very often individuals have absolutely no knowledge of just who might hold information about them. Moreover, they feel vulnerable because of the well publicized cases where privacy infractions or problems have not come to light until well after the fact.

Medical and Social Research

By far the greatest volume of responses to the Discussion Paper came from the medical and social research community. While fully endorsing the need for protection of personal information, almost unanimous concern is expressed about the potentially negative effect of proposed protection measures on medical and social research.

The types of research involved include studies on the continuity and effectiveness of health services, the use of multiple prescription drugs by the elderly, the incidence of serious and fatal diseases such as cancer and heart disease, the outcomes of therapeutic procedures and drugs, environmental effects on health, how families and individuals respond to the changing social and economic environment, etc. This research has important public benefits related to the improvement of health in the community and the ability to make effective decisions in the health and social policy fields.

The actual concern revolves around the fact that if Canada adopts identical principles to those included in the draft EC privacy directives it is believed that the ability to carry out essential research in the public interest could be stifled. The reason is that no exemptions are provided in the EC directives regarding prior consent to the collection and use of personal information, and for the retention of personal information only for as long as it is required for its initial purpose. Therefore, the prohibition of long term storage would make it impossible to track case histories over a lifetime, and the need to obtain consent would present prohibitive logistical and cost barriers.

The submissions from the medical research community provide great detail on the security measures taken to protect personal information. These include: anonymization of personal data by the use of scrambling techniques; locked research areas; computer security systems; oaths of secrecy; approval and enforcement of project protocols by university and provincial bodies; structural separation of research from administrative functions; etc. Also, none of the respondents is aware of confidentiality ever having been breached. Moreover, the focus is not on individual patients but on groups or populations of patients. Therefore, they consider that there is no justification for applying the same restrictions concerning consent, use and retention of data held for research purposes as is proposed for data held for other purposes in the public and private sectors. As one researcher put it " Are we inventing a cure for which there is no disease?".

In overall terms, there is a strong belief, expressed by many respondents from all sectors, that if the various concerns of the general public are not alleviated, the information highway will not be used to its full potential.

HOW TO ENSURE PRIVACY?

The Canadian Experience

Some of the submissions touch on the Canadian experience with privacy legislation, regulations and voluntary codes, by way of background to the current situation

Only six jurisdictions are shown to have effective privacy legislation covering the public sector, i.e. the Federal Government, Quebec, Ontario, Alberta, Saskatchewan and British Columbia. Whereas, only Quebec has legislation governing the private sector. Other federal legislation also has provisions related to privacy. The Telecommunications Act has provisions to protect the privacy of individuals, including the regulation of unsolicited communications. Also, amendments to the Criminal Code and the Radiocommunication Act now forbid the divulgence of intercepted radio-based telephone communications. Furthermore, the new Bank Act, Insurance Companies Act and Trust and Loan Companies Act permit regulations to be made governing the use of information provided by customers. In addition, all English speaking provinces, with the exception of New Brunswick and Alberta, have some form of legislation protecting consumer credit information.

At the federal level, there is very little protection of privacy by formal regulations. Recent decisions of the CRTC have restricted the use of ADADs and limited the use of junk facsimiles and live voice calls for solicitation purposes. In addition, it has prohibited the use of pre-recorded or computerized calls for solicitation purposes and has made clear that telephone companies can, on two days notice, cancel the service of ADAD users who violate this provision. In approving "name display service", it has also directed telephone companies to provide free per-call blocking of the display on a universal basis. Finally, it has indicated that it will not grant speedy approval to competitive filings of telephone companies if those filings raise privacy concerns. Under the Bank Act, Insurance Companies Act and Trust and Loan Companies no regulations have as yet been established in regard to the use of customer information.

In the private sector, a number of industry associations and businesses have instituted voluntary privacy codes. In the telecommunications industry, the then Minister of Communications issued a set of six "Telecommunications Privacy Principles" in 1992. They were to be implemented by a Telecommunications Privacy Protection Agency made up of representatives of industry and consumer groups. However the Agency never got of the ground for a number of political, economic and practical reasons. The Canadian Direct Marketing Association (CDMA), the Canadian Bankers Association, and Stentor have all issued privacy codes for their members. The cable industry also has embedded privacy

principles within a general set of industry standards that is administered by the independent Canadian Cable Television Standards Council. In addition, a number of individual companies have developed there own voluntary privacy codes.

In summary, however, in spite of the considerable effort put in to these initiatives, many respondents see this as a patchwork approach which is confusing and difficult to understand by the average individual. Nor will this approach address emerging international standards, the dangers of rapidly evolving technologies, or the expectations of the public.

International Experiences

Many respondents see international experiences as being the root from which Canadian privacy endeavours have grown and as a model upon which future endeavours can be based.

In the 1970s many European countries had adopted privacy legislation which often was incompatible among the various countries. Accordingly, the OECD issued a set of guidelines in 1982 on the "Protection of Privacy and Transborder Flows of Personal Information" for adoption by its members. These guidelines which established basic privacy principles, also provided for restriction on the transborder flow of personal information to countries which did not comply with equivalent privacy protection principles. Much of the public sector privacy legislation in Canada is based on the principles in the OECD guidelines. However, although Canada acceded to the guidelines in 1984, the effect of the restriction of transborder data flow provisions has been negligible because of their voluntary nature. Subsequently, in 1990, the EC drafted privacy directives on the "Protection of Individuals in Relation to the Processing of Personal Data", which are aimed at harmonizing all European data protection legislation to offer common and high levels of protection in order to facilitate trade. The directives will have the force of law if passed by the European Parliament. The latest draft of the directives, which build on the OECD guidelines and principles, take into account practical difficulties experienced with the OECD guidelines and somewhat reduce the rigidity of the earlier provisions. Thus, transborder data flows are allowed to countries which have adequate, rather than equivalent, data protection measures. More importantly, they provide for the protection of personal privacy as a basic human right, cover both the public and private sectors and apply to both automated and manual records.

Since the 1970s the United States has, at the federal level, passed various pieces of privacy related legislation ranging from a general Privacy Act to sectoral specific legislation covering such areas as credit reporting, computer fraud and privacy in electronic communications. However, none of this legislation covers the protection of personal information across the whole of the private sector. Indeed, in 1977 the Privacy Protection Study

Commission explicitly rejected an omnibus private sector data protection law on the European model. It favoured a combination of legislation and non-statutory codes that would be sector specific and thereby more sensitive to the different information-handling practices and the needs of different industries. Moreover, the US legislation has neither oversight provisions nor data protection boards or privacy protection commissions. More recently, however, new studies have commenced in the USA in regard to privacy on the information highway. Similar to this current study by the Advisory Council, they are being undertaken by the National Information Infrastructure (NII) Privacy Working Group, and the National Telecommunications and Information Administration (NTIA). New draft general privacy principles have been developed by the NII and a discussion paper has been issued by the NTIA for comment. In addition, new Telecommunications Bills before Congress also deal with telecommunications-related privacy concerns.

A number of respondents also favourably review privacy experiences in other countries such as Holland, Great Britain, New Zealand, Hong Kong, etc.

Privacy Principles

The response to the Discussions Paper's request for comments on the principles that should form the basis of effective privacy protection has been met by a wide range of responses. Therefore, the specific responses are included, where applicable, in each of the summaries of submissions received, as set out in Appendix A. However, some common threads are discernible.

Basic to the arguments of some privacy and consumer advocates and privacy commissioners is the premise that the right to privacy is a fundamental human right. Stemming from this, is the view that privacy is too important to be left to the whims of the marketplace and therefore privacy protection should be seen as an integral and necessary part of doing business.

The ability of individuals to control their personal information is perhaps seen as the major privacy issue. Such control extends to collection, subject to statutory requirements, as well as to use and disclosure in accordance with fair information practices.

An essential element of control is the question of consent. However, this has different interpretations in different sectors. Generally, the consumer and privacy advocates and privacy commissioners see this as "informed consent". This is interpreted to mean a clear understanding of the reasons for the collection of information and the uses to which it will be put, and being free from any form of "coercion". Many in the business sector also

appear to subscribe to the concept of "informed consent" while not defining it in that manner. Whereas others tend to see consent as being deemed to have been given by the entry into a transaction. Also, whereas privacy and consumer advocates and privacy commissioners see consent as being given by "opting-in", the business sector prefers the concept of "opting-out".

Other principles, based in large measure on the OECD guidelines and the provisions of the federal Privacy Act, include: identification of the purposes of collection; limiting collection to information which is necessary for those purposes; ensuring that personal information is as accurate and up to date as is necessary for those purposes; allowing access by individuals to their personal information, including correction where necessary; and, providing mechanisms for complaints and redress.

Some additional principles have arisen in recent years due to advances in technology and the changing marketplace. These include the requirement for the protection of personal information by security safeguards appropriate to the sensitivity of the information, and the principle that individuals should not have to pay to maintain basic and existing levels of privacy. Related to this latter aspect, there are some differences of viewpoint. Some maintain that consumers should pay for enhanced privacy above the basic level, whereas others maintain that privacy should not be prejudiced by inability to pay. Another principle entails freedom of individuals to choose whether or not to connect to the information infrastructure, to accept or reject services that may affect their level of privacy, and to be free to subscribe to, and be charged for, only those services they wish to receive. However, they should not suffer reduced levels of service because of their choice.

In overall terms, there are not significant differences in views relating to privacy principles between, on the one hand consumer and privacy advocates and privacy commissioners, and on the other hand the business sector. Both groups show strong support for the privacy principles included in the CSA draft model code which are, in the main, equivalent to those set out above.

Some of the submissions also advance principles that should govern the development of the information highway, particularly as it relates to privacy issues. These include the principle that privacy measures must be compatible with the dynamic and often unpredictable evolution of the highway, and that the protection of privacy on the highway must be balanced with the rights of creators to know who is using their intellectual property.

The Public and Private Sectors

Some of the consumer and privacy advocates and privacy commissioners see a relatively new and emerging problem in relation to privacy on the

information highway. This is seen as a blurring of the distinction between information which is resident in the public sector and that which is resident in the private sector. Therefore, contracting-out of more and more public functions to the private sector is expected to have an increasing effect on the privacy practices of the private sector. As personal information in the public sector is passed to the private sector for the fulfilment of these contracts, the public sector will no doubt ensure that its privacy protection obligations are made part of those contracts. In addition, the increasing matching of public sector information with private sector information, such as the matching of data on welfare recipients with bank or financial information to ascertain eligibility, also are seen to narrow the gap. Likewise, in an evolutionary sense, the continued efforts of privacy commissioners and the press in bringing privacy issues to the fore will also have a spillover effect. In fact, one international respondent believes that the abandonment of the distinction between the public and private sector in the latest draft of the proposed EC privacy directives reflects the fact that the increasing flows of personal information between those sectors renders the distinction irrelevant.

Within the private sector alone, further blurring is seen between the individual industries using the information highway. Because of integration of the various media and technologies in a "seamless web", the former clear distinction between telephone companies, cable companies, broadcasters, the press, marketers, etc., is increasingly ceasing to exist. This leads to difficulty in determining where one sector ceases and another commences. Therefore, a potential problem is seen in establishing privacy protection on a purely sectoral basis.

A Level Playing Field

Reference has been made earlier to the patchwork of federal /provincial legislation and regulations, as well as the multitude of different private sector codes across both Canada and all sectors of the marketplace. This results in concerns arising in both private sector groups and the consumer and privacy advocacy and privacy commissioner groups. The problem seen by some members of all of these groups is that if a national privacy standard is not established across Canada, privacy inequities will continue to occur between different individuals, based on both their respective geographical location and the respective business organizations with which they do business. Moreover, some business organizations may be able to achieve discriminatory and unfair marketing advantages. Failure to create a level playing field could possibly lead to the creation of "data havens," whereby the most lenient jurisdictions may attract businesses that seek to evade privacy protection measures Also, artificial legal distinctions would have to be made about where data is "located" when it travels the highway.

Legislation and Regulation

By far the greatest debate and difference in views occurs in regard to whether the preferred approach to privacy protection rests with legislation and regulation or with voluntary codes and standards. Each of these views has its supporters and detractors for a wide variety of quite valid reasons.

The majority of respondents who addressed this issue believe that the government needs to take stronger action to protect the privacy and security of information. While acknowledging the differences in federal/provincial jurisdictions and the difficulty of harmonizing approaches between them, most of the respondents who seek stronger measures believe that additional legislation and regulation, covering both the public and private sectors, is essential. In addition, the 1992 Ekos privacy survey revealed that "compared to a model of pure voluntary self-regulation by business, Canadians strongly prefer a governmental legislative response".

The reasons why legislation and regulation are seen to be required cover a wide range. It is perceived to be the only way to establish a level playing field across Canada and to guarantee an adequate level of privacy protection for the public, free of confusion and regional and sectoral inequities. Moreover, there is a risk that transborder flows of data could be prejudiced if privacy protection measures are not deemed to be adequate under the proposed EC privacy directives. National legislation and standards would meet this requirement. Furthermore, equal legislated national privacy standards for both the public and private sectors would do much to negate the concern related to the blurring of the distinction between information which is resident in the public sector and that which is resident in the private sector. As one consumer advocate indicated, there has been enough discussion and evidence of the inadequacy of voluntary codes over the last ten years that the government must act now and be seen to take a leadership role. Reinforcing this view, is the observation that Canada is one of the few western type democracies that does not have legislation covering both the public and private sectors.

The manner in which legislation and regulation can be implemented also covers a wide spectrum. Starting with the public sector, there are suggestions that the government should "clean up its own shop". As a start, there should be amendments to the Privacy Act. A preamble to the Act would clearly establish the principle that privacy is a fundamental right (this is also seen as a requirement in any additional legislation governing the private sector). There should be a provision for the protection and security of personal information. The undertaking of privacy impact assessments as part of the design process of all new or major revisions to government systems and programs would become mandatory. Finally, a process would be established whereby a standing parliamentary committee would hold hearings on the Privacy Commissioner's Annual Report and the annual reports of government departments, similar to the manner in which

the Public Accounts Committee reviews the Auditor General's Report and the public accounts of individual departments. In addition, a number of respondents call for the government, in assuming a leadership role, to legislate privacy requirements on organizations that fall within the federally regulated private sector and to take all other means within its control that would promote the adoption of privacy measures by the private sector.

In regard to legislating privacy in the private sector, supporters of the proposal tend to favour the establishment, by legislation, of a national framework of privacy standards under which private sector codes would operate and be bound. This would be complemented by an independent and impartial administrative mechanism which would enforce compliance, hear complaints, provide redress and deliver sanctions. A number suggest that such a system could be based on the Quebec Act Respecting the Protection of Personal Information in the Private Sector which is the only privacy legislation governing the private sector in Canada. However, such a view is not unanimous. One private sector institution believes that the Quebec Act does not achieve a balance between the protection of privacy and the free circulation of information which is so necessary in a market economy. However, another indicated that the Act had had little impact on its policies and procedures although it was viewed as "overkill" in some respects. It is also recognized that such legislation would have to be both framed and implemented in the most non-bureaucratic and cost-effective manner possible. This view is reinforced by one British respondent who states that the data registration provisions of the UK Data Protection Act are largely ignored because they are too bureaucratic and fairly meaningless. Also, it is suggested that any legislation should have a phase-in period in order to avoid economic upheaval in areas such as the direct marketing industry which employs thousands of Canadians. Other suggestions for such legislation include provision for "whistle blowing" against organizations engaged in illegal activities, and the recognition of joint culpability on the part of both senders and receivers. Furthermore, the government is urged to quickly enter into discussions with the provinces with a view to harmonizing both public and private sector legislation across Canada.

Opponents of legislation and regulation see a number of problems in taking the legislative route. Legislation is seen as too blunt an instrument which would be inflexible and be incapable of reacting to the accelerating changes and needs of both technology and the marketplace. Moreover, it is also seen as being capable of inhibiting new initiatives and prejudicing investment in these areas. In this regard, the fact that business requirements and technologies differ from one sector to another would only compound the problem. The time it would take to secure agreement between the federal and provincial jurisdictions also is considered to be a major factor against legislation. Furthermore, some believe that voluntary codes and standards are only in their infancy and have not yet been given a chance to prove themselves, therefore legislation should only be used as a

last resort. Legislation and regulation also are seen as going against the current trend to deregulation in the global marketplace, as requiring additional public funding in a time of fiscal restraint, and as possibly leading to "micro-management" of the marketplace.

In general terms, consumer and privacy advocates and privacy commissioners favour legislation, whereas the private sector is against it. However the picture is not completely black and white. One technology association supports legislation in order to guarantee consistent and appropriate levels of privacy protection. Whereas, a telecommunications company believes that the regulated telecommunications industry should be exempted from any future legislation because it is already governed by the privacy provisions of the Telecommunications Act. Other private sector organizations would not be against legislation if it was shown, after a reasonable period of time, that voluntary codes and standards were not working, provided that it recognized marketplace realities.

However, the radio-telecommunications industry is strongly in favour of technology- specific legislation. It believes that the government should move quickly to pass legislation to make it an offence to intercept radio-based telecommunications and to generally prohibit the manufacture, importation, sale and distribution of scanners capable of monitoring radio-based telephones, including cellular phones.

In regard to the question as to whether adequate privacy protection can be provided through provincial or sectoral legislation, there are somewhat conflicting views. However, there seems to be general acceptance that such a course would not be sufficient by itself. Strong opponents of legislation are opposed to it whether it be federal, provincial or sectoral, while others agree that, if legislation is to be enacted, it must be based on national standards in order to ensure a "level playing field. There is equal concern about "balkanization" occurring coupled with the establishment of "data havens". In summary, in any move towards legislation, discussions and coordination with the provinces are considered to be essential.

Voluntary Codes and Standards

The main benefits of voluntary codes and standards are seen to be their flexibility and adaptability. It is pointed out that different sectors are engaged in different business practices and utilize different technologies. Therefore, flexibility allows them to customize their privacy practices to the specific nature of the business and to the needs of their customers. Also, they can more quickly adapt and be more sensitive to changes in business practices, as well as to evolving technology and consumer privacy concerns. Moreover, regular reviews can be undertaken to assess the effects of changing circumstances. Voluntary codes also can be national in scope, providing a level playing field across individual sectors, thus avoiding

the problems of different federal/provincial jurisdictions. Additional advantages are also linked to the fact that they can be less costly to operate and responsibility and costs can be focused within the organization. Furthermore, they can raise the profile of privacy within an organization and help to educate the public, thereby building the confidence of consumers while allowing them to fully participate in the benefits of the information highway.

Voluntary codes and standards can be implemented in many ways, each tailored to the particular needs of a sector. They can be made mandatory on the members of a given sectoral association, as with the Canadian Direct Marketing Association code, or they can be incorporated in the confidentiality Terms of Service approved by the CRTC, as with the regulated carriers governed by the Telecommunications Act. In addition, the adoption and implementation of voluntary codes can be made necessary by peer pressure, compelling competitive interests and consumer demand, whereby consumers will "vote with their feet" if they are not satisfied that their privacy concerns are being met.

One of the most significant developments in voluntary codes at the present time is seen as the CSA draft model privacy code which is strongly supported not only by the private sector but also by consumer and advocacy groups and privacy commissioners. It contains ten principles for the protection of personal information (see Appendix B) which are based on the OECD guidelines. Its main advantage is that it is being developed by a consensus of views emerging from the CSA Technical Committee on Privacy, which is made up of representatives from governments, privacy commissioners, privacy and consumer advocates, labour, and the private sector. Also, it could be the basis for a national standard against which other voluntary codes could be measured. Equally, it could provide a standard against which the international community could judge the adequacy of Canada's personal information protection practices. However, the manner in which it can be implemented is still under study.

The main objection to the use of voluntary codes is that they are voluntary and, like chains, they are only as strong as their weakest links. Moreover, they are sometimes only half measures which are not fully responsive to consumers privacy concerns, in that they do not always include the full range of fair information practices. Often they do not include provisions for independent arbitration, provisions for monitoring and measuring performance, provisions for sanctions and penalties, or adequate provisions for complaint and redress. Furthermore, they sometimes lack effective administration at the corporate and sector levels, and may be tailored more to business practices than to the protection of privacy. Also, their coverage within a sector may often be inadequate and inconsistent. Consumers may lack awareness of the existence of voluntary codes and often have little input into their development. Finally, they may not meet the "adequate" standards of privacy protection required under the EC draft directives.

Although most of the support for voluntary codes and standards comes from the business sector, consumer and privacy advocates and privacy commissioners see voluntary codes and standards as having an important role to play, provided they are governed by overarching legislation. In reaching this view, they are cognizant of the shortfalls of legislation, e.g., rigidity, the time taken to implement, etc., as well as the benefits of voluntary codes, e.g. flexibility, responsiveness to particular needs, etc. In this sense, voluntary codes are seen as being a first step towards data protection, as being deserving of legislative back-up if they are to be really effective, and as being an acceptable part of the solution if they can be demonstrated to work. The fact that they can help to raise employee awareness, is also acknowledged. Furthermore, some members of the consumer and privacy advocacy and privacy commissioner groups suggest that they can help industry to "get up speed" before legislation is introduced and, in doing so, can guide legislative drafters on sector specific issues and means of implementation.

Technological Solutions

There is general agreement that technological solutions have a part to play. While many maintain that the accelerating pace of technology is a threat to privacy, it is also acknowledged that new developments in technology can now allow better privacy protection features to be built in from the outset. This latter factor is seen as being very important; supporting the view that before new technology and systems are developed, privacy impact assessments should be built in as an essential part of the development process. In fact, one respondent has developed a step by step process as to how this can be accomplished and another provides suggested rules for evaluating the privacy impacts of emerging technologies. While many see such impact assessments as adding to the cost of new systems and possibly delaying their development, others see them as possibly avoiding future costs by eliminating expensive retrofits to incorporate privacy protection functions at a later date. Here, the need to add free call-blocking as a requirement for the introduction of name-display by the telephone companies is given as an example, as is the abandonment of the Lotus Marketplace: Households product.

The question of whether the information highway should be designed to provide high levels of privacy protection and whether it will slow the pace and raise the cost of innovation is also addressed by many respondents. Built in security measures are seen as a key in this regard. Generally speaking, it is acknowledged that there is a clear responsibility for basic protective measures. However, these measures should be proportionate to the privacy issues associated with each particular application. For instance , the Internet requires little built-in protective measures, whereas banking transactions and access to medical records require a high degree of protection. Between these two extremes, various levels of protective

measures could be instituted, with the consumer having freedom to choose, sometimes at added cost. Beyond the normal protective measures, such as the use of access codes, new developments in encryption, such as "public-key" encryption, and the use of smart cards are seen as additional measures. Also, the implementation of digital technology is seen as a significant contribution. Furthermore, it is suggested that the government encourage new technology in this area and support research and development in order to provide new opportunities for Canadian industry. On the question of whether such measures will be more costly or will inhibit innovation, the prevailing view is that this will not occur provided that such measures are not too excessive. However, as one privacy commissioner suggests, the costs, in terms of loss of human dignity and autonomy, are too great not to require high levels of privacy to be built in. In the final analysis, the private sector recognizes that if consumers do not have confidence that the highway will protect their privacy interests, it will not be used to its fullest extent.

On the question of how Canadians can become better involved in the design of potentially privacy-threatening technologies and services, there is a wide variety of views. It is pointed that, at the present time, consumers already have the opportunity to become involved. CRTC hearings on the introduction of new regulated telecommunications services is given as one instance. Participation and advice on the development of new CSA technical standards is given as another. Nonetheless, there is strong support from consumer and privacy advocates and privacy commissioners for public participation in the development of all significant new and potentially privacy threatening systems. Two private sector organizations also support public participation on the basis that consultation can forestall delays and possible litigation. An example is given in relation to the current debate on whether fibre optic services should go right into the home or whether they should terminate 100 metres away and then be transmitted by wireless communication. The latter option is less costly but is fraught with privacy protection implications. In any event, advance consultations with consumers and/or privacy commissioners are seen as potentially beneficial to private business, as long they are relatively informal and not the subject of long drawn out public hearings.

Consumer Education

There is wide recognition of a lack of awareness and confusion among the public in regard to the benefits and services that are and will be available on the information highway. This is coupled with an equal lack of awareness concerning their privacy rights, how to obtain those rights, the consequences of providing personal information, and the protective measures which are available. This leads to vague but real concerns which could prejudice the success of the information highway. Therefore, there is widespread agreement that education of the public on these matters is both

essential and urgent in order to reduce concerns and because of the rapid growth of the highway. In addition, it is recognized that both employees and businesses need to be educated on their responsibilities in regard to privacy protection.

A general consensus is evident that both governments and business have major responsibilities in this area. Most private sector organizations indicate their commitment. Many are already engaged in education programs, not only for their customers but also for their employees. Moreover, consumer and privacy advocates and privacy commissioners indicate their willingness to become more involved, provided funding and resources are made available. In addition, the media is also seen as having a significant role to play. However, it is also recognized that consumers themselves must take the initiative to absorb educational materials provided to them, to shop around for the best balance of services and privacy protection, and to understand their own responsibilities in regard to privacy matters. Equally, businesses must also take the initiative to inform customers of potential privacy problems related to their products and services and not hold back until a crisis occurs.

The tools available are seen to be many and varied. Everyday business practices, coupled with the publicizing of industry codes, will be powerful mechanisms, as will the publicizing of the CSA model privacy code. Massive advertising campaigns are not recommended, although periodic public awareness campaigns, which could take many forms, are recommended. The use of information centres, including public and academic libraries, for the distribution of materials and brochures also is considered to be another avenue. Brochures and publications can be directed at different audiences, including the public at large, schools and universities, and customers of businesses. Other suggestions include a privately funded national toll-free privacy "hotline" for consumers and the inclusion of a confidentiality clause in all contracts.

CONCLUSIONS

Concerns

It is quite that evident that there is a wide range of real public concerns on privacy matters which, if not addressed quickly, could escalate to the point that the effective functioning of the information highway could be jeopardized.

How to Ensure Privacy?

There is a significant divergence of views between the majority of members of the private sector and consumer and privacy advocacy and privacy commissioner groups in regard to the relative merits of legislation and voluntary codes. However, there also is a pragmatic and conciliatory approach to these differences which makes a compromise achievable.

No single approach to the resolution of the problems is viable. Therefore, a combination of the approaches outlined in the Discussion Paper is most likely to succeed because they are inter-related and mutually supportive.

In order to achieve comprehensive solutions to the various problems identified by respondents, within the minimum possible time frame, a well-coordinated plan should be developed.

The following are potential elements of a plan which the Advisory Council may wish to consider.

- The establishment by legislation of a national framework of privacy standards, probably based on the CSA model privacy code, under which private sector codes would operate and be bound.
- Revisions to the federal Privacy Act to overcome its current shortcomings, including a revised preamble, provision for the protection and security of personal information, and provision for the establishment of privacy impact assessments within the public sector.
- Development of a program to reinforce, strengthen and update the application of privacy requirements within the public sector.
- Early discussion with the provinces to implement national standards on a country-wide basis.
- Development of legislation to make it an offence to intercept private radio-based telecommunications, and to generally prohibit the manufacture, importation, sale and distribution of scanners capable of monitoring radio-based telephones, including cellular phones.

- Development of a program to systematically promote the development of private sector codes based on the CSA model privacy code.
- Creation of a joint government/industry program to promote and support the development of privacy protection technologies.
- Promotion of consultations between industry/government, consumer groups and privacy commissioners on the development of significant and new potentially privacy-threatening technologies and systems.
- Development of a joint industry/government privacy education program in consultation with consumer groups and privacy commissioners.
- Establishment of consultations between government and the medical and social research groups to resolve the apparent dichotomy between the protection of personal information and the need to carry out medical and social research necessary to promote the public good.
- Development by the government of a standard privacy protection clause for all contracts or agreements involving the transfer or exchange of personal information with all institutions outside of government.
- Issuance of a public announcement after adoption of the plan and ministerial approval.

Failure to Address the Problem

Failure to address the major problems identified by respondents could be followed by increasing public privacy concerns, coupled with avoidance of the use of the information highway. Also, it might lead to Canada's privacy protection standards being considered inadequate under the European Communities' privacy directives.

Appendix A

PRIVACY AND THE CANADIAN INFORMATION HIGHWAY

SUMMARIES OF SUBMISSIONS RECEIVED

Appendix A

TABLE OF CONTENTS

SUMMARIES OF SUBMISSIONS RECEIVED

INTRODUCTION

The 76 submissions received have been broken down into eight different categories of respondents. These categories and the relevant number of responses in each are as follows: Medical and Social Research (21); Individuals (11); Telecommunications and Technology (12); Privacy and Consumer Advocates (11); Financial, Credit and Direct Marketing (5); Privacy Commissioners (4); Government (4); Miscellaneous (8).

Short summaries of the relevant details of each of the submissions are set out below. They are listed under the categories and in the order shown above. Because the actual submissions (including attachments) varied in length from one page to 60 pages, considerable editing has had to be done in order to achieve manageable proportions. In general, the editing consists of the elimination of duplication and examples provided to illustrate points made in the submissions. However, the main elements of issues raised have been preserved, together with reasons for raising the issues. In this manner, it is believed that the more important aspects of each submission have been retained.

For ease of comparison, each submission has been summarized and edited to comply with the general format of the main report. Therefore, the layout consists of a General Overview and, where applicable, comments on Privacy, Privacy Concerns, and Means to Ensure Privacy. Under Means to Ensure Privacy, where respondents have made specific comments on the Approaches set out in the Discussion Paper, these are shown against the relevant Roman numerals below. Equally, where specific Answers to Questions have been provided, they are shown against the relevant Arabic numerals. As well, where applicable, Specific Proposals and Recommendations, stemming from the four main approaches included in the Discussion Paper, also are shown.

Approaches

I. Legislation and Regulation

II. Voluntary Codes and Standards

III. Technological Solutions

IV. Consumer Education

Answers to Questions

1. What principles should form the basis of effective privacy protection?

2. 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?

3. Is a national level of privacy protection needed, or can adequate privacy protection be provided through provincial or sectoral legislation?

4. In which circumstances might voluntary privacy guidelines developed by business be appropriate?

5. 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?

6. How can Canadians become better involved in the design process for potentially privacy-threatening technologies and services?

7. 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?

Patricia Baird, MD, CM, FRCPC, FCCMG

Patricia Baird is a Professor at the University of British Columbia.

Professor Baird believes that the right to control information about oneself is of fundamental value in Canadian society and needs to be respected. However, society also has an interest in using the information in medical records for research into pattems of illness or disability, the use of harmful procedures, and drugs and to evaluate the outcomes of treatment. Canadian citizens rely on governments to protect their safety in this regard. Therefore access to such information, record linkage and other research techniques are essential. She firmly believes that it is possible to protect individuals' privacy and at the same time reap the benefits of these types of research which are a societal need.

Specific Proposals and Recommendations

Privacy legislation and regulations should be designed to permit information linked to individuals to be linked, aggregated and analyzed for health purposes.

Dalhousie University

The submission is made by Dr. John Ruedy, Dean of the Faculty of Medicine and Chair of the Advisory Committee, Population Health Research Unit.

The Research Unit administers a database of health system encounters which is used in research to enhance the efficiency and effectiveness of the Canadian health system. The research requires the use of longitudinal person specific information and its linkage from different programs and sources. Because privacy is of great importance to the research community, all data are rendered anonymous by encryption at various levels of program and source. Furthermore, principles and procedures have been developed that protect against inadvertent disclosure of small cell data and all research projects are screened by a research committee and referred to a university ethics committee, when appropriate. Thus, the confidentiality of individual records is protected while allowing information to be used for legitimate and important research purposes.

Concern is expressed that future standards requiring consent for any use of personal information or that limit collection and retention of data might prohibit research activities, thereby preventing the public benefits of such research. A balance of interests between privacy needs and the need to optimize the use of scarce resources in the health system must be achieved.

Specific Proposals and Recommendations

Information about individuals, rendered anonymous to others and used for approved systematic analysis, should not be equated with personal information in future privacy legislation.

Emerging policies must recognize the public benefits of access to individual data for health research purposes.

Allan S. Detsky, MD, PhD, FRCPC

Allan Detsky is a National Research Scholar and Professor of Health Administration and Medicine at the University of Toronto.

Professor Detsky is concerned that potential privacy legislation may not allow researchers to utilize administrative data sets for use at a later time in research. Such research will help policy makers decide on resource allocations which are essential to resolve the crisis in health care costs in Canada. Use of administrative data is crucial to research and requires file linkage in the absence of explicit consent. In all cases of which he is aware, patient identifier information has been removed and he believes that there is no way that the identity of individuals could be compromised.

Canadian Institute for Advanced Research, Population Health Program

The Population Health Program is a network of senior researchers from Canada and abroad, based in universities and other institutions, e.g. Statistics Canada. They are working together to advance understanding of the fundamental factors that underlie the marked disparities in health among sectors of the Canadian population, and also are engaged in research on the functioning of the health care system.

Research by members of the Program, and by many other epidemiologists and social scientists, relies heavily on access to provincial health care databases and on the merging of health care and socio-economic data to answer key questions about the health of Canadians and the use of the health care system. This requires the assembly of data from numerous sources over a long period of time because the trajectory of health in individual patients and the use of health care is not a "one off" event. Whether the decline of hospital inpatient capacity and use results in inadequate care is a typical question to be answered by this type of research. This research is conducted without compromising the privacy of individuals by using anonymous linkage of patient-specific data. Also, Program members have worked closely with federal and provincial privacy commissioners to secure permission for this anonymous linkage. Moreover, all research is reviewed by the appropriate university ethics committee.

Concem is expressed that some of the lines of approach suggested in the Discussion Paper, while responding to important privacy concems, could have devastating side effects and bring to a halt some of the most promising forms of health research currently underway in Canada. "The physician whose recommendations showed no concem for side effects would be justly criticized for focusing on the disease but placing the patient at unnecessary risk". Concem is also expressed that adoption of the European Community draft directive on the confidentiality of data, particularly those relating to consent, proposed uses and time limits on retention, will terminate such research with major public health implications. Where there is significant justification for research purposes and adequate protection of data, blanket restrictions on the preservation, linkage and use of personal data would go far beyond what is necessary to protect individual privacy and would be contrary to the public interest.

Specific Proposals and Recommendations

Undue restrictions should not be allowed to jeopardize the fruitful research environment.

Institute for Clinical Evaluative Sciences in Ontario (ICES)

ICES is a non-profit research corporation funded by the Ontario Ministry of Health. Its mandate is to carry out research that will improve the quality, efficiency and effectiveness of physician and allied professional services in Ontario. The submission is made by C. David Naylor, MD, DPhil, FRCPC in his capacity as Director of Clinical Epidemiology at the Sunnybrook Health Science Centre of the University of Toronto and as Chief Executive Officer of ICES.

Use of a wide variety of health-related data and its linkage, using unique identifiers, is a comerstone of health research with tangible benefits for the Canadian public. There is a distinct difference in intent from such usage by for-profit enterprises that package and resell data, by insurance companies seeking to assess an individual's insurability and by govemment itself. Health researchers work from academic centres, have their work reviewed by ethics boards, and have a keen awareness of its privacy implications. Although health research follows individual patients over a period of time, the focus is not on individual patients but on groups or populations of patients. Even though individuals fear abuse of information by service providers and employers, the Institute believes that Canadians are willing to support limited access to health data by health researchers provided that confidentiality is protected.

Methods used to ensure confidentiality of data include scrambling of patient identifiers, shredders, and confidential waste disposal procedures. As well, staff sign a stringent confidentiality agreement. Concem for privacy is

evidenced by the attachment of a working paper published by the Institute which is a review of literature on "Ethics and Health Services Research".

Concern is expressed about some aspects of the Discussion Paper, particularly possible restrictions on the use of single numerical identifiers. Without such identifiers, researchers are unable to make sense of how patients move through the health care system. For instance, research on a particular health risk may involve review of data on tens of thousands of patients in order to determine whether the risk should be of concern. Concern is also expressed that adaptation of the European Community draft directives, particularly in regard to consent, could prejudice the validity of research results. Refusal of consent by a large number of patients, based on a misunderstanding of the extensive privacy safeguards used by researchers, could put in doubt the generalizability of the rest of the data.

Specific Proposals and Recommendations

ICES offers further consultations between health researchers and other stakeholders and citizens in order to ensure that standardized operating principles can be devised to meet legitimate privacy concerns.

Robert C. James, MA, MSc

Robert C. James is a doctoral student in Community Health Sciences at the University of Manitoba.

While acknowledging that data protection is an important policy goal, he expresses concern that the uncritical application of data protection and privacy rules, which are generally designed to restrain government and business, may frustrate or foreclose on important research and policy development. Particular concern is expressed that a strict reading of the Discussion Paper could lead to a situation not dissimilar to that currently ongoing in Europe. In that respect, the draft privacy directives of the European Community have been forecast to have a chilling effect on the practice of public health, due to the requirement for consent and limitations on the secondary use of data. Such effects in Canada would have important negative social costs and are avoidable if the important role of medical and social research is recognized. The use of individual-level linkable data is essential to such research and the requirement for consent leaves open the potential for misleading bias that could invalidate research.

Specific Proposals and Recommendations

While not arguing for a blanket exemption for researchers, he urges the Advisory Council to work with research communities to define appropriate standards for the development, maintenance, use and disposition of individual-level data. The issue of consent and secondary use must be specifically addressed.

Manitoba Cancer Treatment and Research Foundation

The Manitoba Cancer Treatment and Research Foundation, which operates the Manitoba Provincial Cancer Registry (MPCR), has a provincial legislative mandate (a copy of the pertinent legislation is enclosed) and has operated for over seventy years. One of its primary purposes is the support of research in cancer.

The Foundation has set out eight principles that support privacy. It also supports legislation that recognizes both the public and private benefits of collecting and recording personal information, and supports voluntary standards in combination with legislation. It believes that technology may be a part of the solution and that there a clear need for consumer education.

It expresses concern that it should be recognized that epidemiological research has assisted in reducing the incidence of or eliminating disease. Moreover, the collection, retention and linkages of individual information permits the delivery of many public benefits including education, social services and health care. Concern is also expressed that provincial cancer registries continue to be available for ongoing epidemiological and health care evaluation research.

The MPCR follows strict guidelines in the release of any data and the approval of the MPCR Access Committee is required for the release of any information that might identify individuals. Also, specific approval must be obtained from the Access Committee, with a thorough review by the University of Manitoba, Faculty of Medicine Ethics Committee, if personal contact with registrants is requested. The MCTRF takes very seriously its responsibility of maintaining the utmost privacy and confidentiality of information stored in the MPCR.

Approaches

I. Legislation ought to recognize the difference between information that is collected for the private good and that for the public good.

II. Voluntary standards, properly applied and enforced, can improve the overall response to changing public opinion, provide a feasible option for ongoing monitoring, and improve the quality of decisions made.

III. Electronic locks (access, encryption, passwords) are some of the fundamental tools in providing data security.

IV. Consumers need education to understand what the technology is capable of , the guidelines and legislation that permit the use of personal information, and the existing safeguards.

Answers to Questions

1. The following eight principles are introduced.

   - Information about an individual is the property of that individual.
   - Individuals have the right to enter into commercial contracts with their information.
   - Commercial transactions based on an individual's characteristics (age, health, etc.) must be limited to information gathered with the consent of the individual.
   - Society has a responsibility role to ensure the likelihood of fair transactions which are free of coercion.
   - Society, through its governments and agencies, has an obligation to provide bonafide public benefits.
   - Society has limited rights to information describing both society as a whole and individual members.
   - Individuals have the right to fair compensation for the use of their Information.
   - Society has an obligation to protect an individual's privacy and anonymity in the collection of data used in the provision of a public good.

2. Legislation must be in place to protect individuals from financial loss or personal damage as a result of the use of unauthorized personal information and to restrict what information can be used in private transactions. It must provide a framework to ensure that information sought is fair and reasonable, does not violate an individual's privacy, and is only used for the purposes for which it was collected. Any newly formulated privacy regulations need to recognize and reflect existing and effective safeguards, the existence of duly constituted professional bodies with codes of ethics, and long-standing institutionalized policies governing confidentiality of health information records and ethic committee/peer review.

3. While national standards are required, they must permit suitable local freedoms. National protection is also required to permit inter-provincial sharing of data while protecting privacy. Epidemiological and health evaluation research often requires large populations for reliable results and the only solution is to do such work at the national level.

4. Voluntary guidelines have preceded specific legislation in many areas and many organizations and professionals have codes of ethics which are open and receptive to public scrutiny. Also, the use

of voluntary standards permits ongoing education and assessment. Moreover, to be effective they must be reviewed by third party individuals or outside organizations. It would be inconceivable that legislation and policy alone could achieve the same level of privacy and confidence that can be achieved in combination with voluntary standards.

5. Clearly the cost of security always impacts the cost and convenience of innovation.

6. Canadians can become better involved by establishing principles and guidelines that dictate the appropriate principles and rights of privacy.

7. Both governments and agencies have the responsibility to promote the potential benefits, past benefits and current work, while at the same time ensuring that the public understands the watchdogs, the ombudsman and the security. There also needs to be clear education on the laws which are there to protect consumers, and to permit them to make informed decisions. The greatest risk the public faces is not having suitable recourse simply out of lack of knowledge or available processes.

Specific Proposals and Recommendations

Where there is a bonafide public benefit in using information that does not inflict undue cost on the individual, then that use should be clearly permitted, if not encouraged.

There must be a public watchdog and/or an ombudsman to address public concerns and to provide an avenue outside the legal system.

Judith Maxwell

Ms. Maxwell submits her comments from the perspective of a social researcher. Her primary concern is to ensure that Canada retains the capacity to use administrative files to observe the way in which families and individuals respond to the changing social and economic environment. This creates an essential foundation for sound public policy decisions, for effective evaluation of government programs and policies, and has an important bearing on reforms to social and economic policies. In short, it is a way to keep governments accountable and to help them be responsive. Moreover, it helps the democratic process if people understand their fellow citizens.

Information required is derived in two ways, by linking administrative and statistical files at a point in time, and by tracking developments in an administrative file over time. By both linking and tracking a file over time,

an even more powerful analytical base is created. This kind of research is affordable compared with the astronomical cost and time delays involved in conducting surveys.

A balance is required is required between the many interests of society. Therefore, it is essential to keep the interests of the research and policy making communities as part of that balance. In doing this, access to administrative files should never be permitted without a careful evaluation of the merits of the research, and their linkage must be shown to generate a significant public good.

It should be possible to write privacy rules that meet the standards put forward in the Discussion Paper. However, the kind of measures mentioned in the document would pose insuperable barriers to social research, i.e. removal of all identifiers would make linkage impossible, prohibition of long-term storage would make it impossible to track a case history over a lifetime, and the need for explicit consent would present prohibitive logistical and cost barriers.

Specific Proposals and Recommendations

The responsibility for linking files and maintaining the data could be entrusted to an independent agency with the technical capacity and political credibility, e.g. Statistics Canada.

The Advisory Council should search for regulations that would permit the new technologies to generate some social good from file linkage.

McGill Health Services and Outcomes Research Group

The Group consists of professors and researchers in the Department of Medicine, Department of Epidemiology and Biostatistics, School of Physical and Occupational Therapy, and the School of Occupational Health at McGill University.

In summary, the Group is greatly concerned that increasingly restrictive rules for access will limit valuable health research and will not serve the public interest. Ethics review boards and provincial agencies now regularly scrutinize data use and the security of health research programs. It is believed that these procedures duly protect privacy while at the same time generating important information that protects public health.

The Group is addressing only one aspect of the Discussion Paper; access to health services data by researchers. Its concerns relate to equating privacy protection problems that arise from access to data collected for commercial purposes to those that arise from access to data in the health related field. The commercial and health fields are completely different, made up of different players and are governed by different codes of

conduct. To have one set of rules for two completely different sets of information is likely to lead to comprises, something that potentially puts too many restrictions on one group while not enough on the other group. In the health field researchers are analyzing information about health states not about people. This is the key difference between commercial and health related activities.

Various examples are given of the important public benefits which arise from health related research such as the continuity and effectiveness of health services, the extent of multiple drug use among the elderly, etc. Also, the need for various forms of privacy protection in relation to health related research is questioned. The need for prior consent is seen as leading to increased administrative costs during a time of declining patient services. The use of personal identifiers and linkage between databases is necessary for research on serious and fatal diseases like cancer and heart disease. The retention of data for long periods is cost effective to enable data to be used to answer multiple health questions that might arise long after the data was originally collected.

High levels of security are seen as being much more important than restricting access and linkage. Of importance in this area are the scrambling of individual identifiers, locked research areas, computer security systems, adherence to codes of ethics, and the protocol for individual research projects imposed and enforced by third parties. Equally, researchers are independent of administrative bodies which may have a vested interest in both collecting and analyzing data. Researchers only analyze data to answer important public health questions and have the necessary training both to correctly identify the question and to reject invalid data. Thus, the public is protected by this independent and professional examination, and from incorrect policy decisions that could be both costly and dangerous for persons needing health care services.

Medical Society of Nova Scotia

The Medical Society of Nova Scotia is a Division of the Canadian Medical Association.

The Society strongly supports the conduct of population based health care studies and believes it would be a loss of incalculable dimensions if the capacity to conduct these studies were to be comprised. Support would be given to any policy that would allow the use of data about individuals to be rendered anonymous and used for systematic research.

Specific Proposals and Recommendations

Information handled in an anonymous manner for systematic research should be specifically excluded from any definition of personal information in any future privacy legislation.

Cam Mustard, ScD

Cam Mustard is a Member of the Faculty of the Manitoba Centre for Health Policy and Evaluation, and an Assistant Professor of Community Health Sciences in the Faculty of Medicine at the University of Manitoba.

As a general commentary, Dr. Mustard found the Discussion Paper to be inadequate relative to issues concerning health information and he raises four such specific areas.

- The consequence of a legislative requirement to obtain individual prior consent which can impair, if not destroy, a research function which provides immense social and individual benefits, is not recognized or acknowledged.
- Given the substantial history of the use of person-level health information for statistical and research purposes, both the surveillance of disease and the monitoring of health system effectiveness and efficiency have become fundamental functions in Canadian society, and are no less important than the protection of privacy.
- The importance of voluntary privacy protection precedents in this country concerning the use of person-level health information for research is not acknowledged and is an unacceptable and distorting omission. These precedents, which stem from the belief that preservation of individual privacy is as important as the pursuit of any specific research project, are evidenced by a wide range of protective measures. These include anonymization of individual-level data, prohibition of reporting research findings at the individual level, structural separation of research from administrative functions, substantial computer security systems, routine review of all research activities by both government and scientific oversight bodies, and confidentiality agreements with all employees which provide for disciplinary actions.
- Failure to distinguish between generalized public apprehension concerning privacy and the consistent and emphatic public support for health research. Currently the National Population Health Survey is reporting consent rates above 90%.

In the interests of contributing further to these issues, Dr. Mustard encloses a 1990 report to the National Task Force on Health Information on

"Implications of Privacy and Confidentiality Concerns on the Use of Health Information for Research and Statistics". The report prepared by a project team led by Louise Desramaux of Statistics Canada is authored by Professor David H. Flaherty and deals in great detail with the history and background of 14 separate privacy concerns and issues, seeks to explain them and, where possible, identifies ways of responding to them. The concerns, particularly of privacy advocates, relate to: the array of administrative and statistical databases and the extent of record linkages; equal concern about statistical and administrative matching; the spread of unique identifiers; the need for informed consent for secondary uses of personal health information; the use of identifiable statistical data for administrative purposes; the risks of unintended release of identifiable information; and, the fact that statistical data are often centralized, kept for long periods and not always anonymized. Moreover, the report highlights: the need for privacy advocates and the general public to recognize the fundamental need for, and existence of, a clear functional separation between research/statistical uses and administrative uses of personal data; the support of privacy advocates for general provincial data protection laws across all provinces in Canada and for specific sectoral laws for health information in the public and private sectors; the lack of general understanding by the general public and privacy advocates that personal information provided to Statistics Canada is kept strictly confidential; caution on the part of privacy advocates in recognizing the desirability of enhanced and essential health information which must be based on statistical record linkages; the acknowledgment by privacy advocates that technical solutions can and should preserve confidentiality; and, the fact that response rates in health surveys are very high, suggesting that the public understands the central importance of health knowledge. Professor Flaherty sees potential responses to these concerns and issues as including the needs for: consultations between the research/statistical community and proxy groups e.g. privacy commissioners, consumers associations etc.; continuing education by the research/statistical community about the serious work in which they are engaged, the careful data protection measures they follow, the potential problems with response rates and public relations that they face, and the fact that statistical/research linkages can be undertaken in such a controlled way as to pose few real threats to privacy interests; provincial legislation to restrict the use of health-related specific identifiers to health-related purposes in both the public and private sectors; legislation, policies and practices to enshrine the existence of clear and functional separation between research/statistical uses and administrative uses of personal data; ensuring that informed consent for secondary uses of personal is recognized as a potential blockage to an enhanced health information system; actively promoting the enactment of general data protection legislation for the public sector in all provinces; and, endorsing the strengthening of specific data protection legislation for health information in both the public and private sectors.

Specific Proposals and Recommendations

There must be a balance between private and public interests concerning privacy protection issues in health research. In part, this can be achieved by: specific recognition of the high level of public support and commitment to health research, including inference of public consent to the use of individual health information in health research; the implementation of legislation providing criminal prosecution if person-level health information is disclosed by researchers or research organizations; and, mandating the existing oversight functions of public and scientific bodies in any new privacy initiatives.

Howard B. Newcombe

Mr. Newcombe states that the idea that we have a "right to be left alone" and to veto any use of our personal information has strong personal appeal but does not reflect what people really want. While wanting strict confidentiality, they also expect protection, services and benefits of many kinds that depend on personal information. He states that currently cancer registries are under threat in Europe from impending "privacy" legislation and that the same threat has been repeated publicly in Ontario. While nobody disputes the need for confidentiality, let us not be misled by the seductive political appeal of an unrealistic and harmful view of "What is Privacy?".

Noralou P. Roos, PhD

Noralou Roos is the Director of the Manitoba Centre for Health Policy and Evaluation, a Professor of Community Health Sciences in the Faculty of Medicine at the University of Manitoba, a National Research Scientist and an Associate of the Canadian Institute for Advanced Research. She is a researcher who has worked with data banks containing information on health contacts for the past 20 years.

In general, Dr. Roos is concerned that Canada might follow the lead of the European Community (EC) in attempting to adopt standards so restrictive as to threaten important research efforts which can benefit the public.

She attaches copies of articles in various medical journals that express the concern that proposed EC standards, as well as the views of many Canadian privacy advocates, could threaten valid epidemiological and health care studies, in such areas as cancer and heart disease research and the effective distribution of health care services.

In particular, she is concerned that the proposed EC standards include provisions whereby: personal data should be kept in identifiable form only as long as required for the purposes for which they were recorded;

processing of data on health is prohibited unless the subjects concerned have given their written consent; and, linking of records across data bases is prohibited without the explicit consent of individual patients.

She states that administrative data, e.g. used for the paying of physicians and to record who is treated in hospital, are invaluable sources to investigate questions of public health, etc. Such research requires the linking of records for thousands of individuals but none of the research files contain names or addresses nor has any of the research resulted in patients or physicians being identified. Dr. Roos attaches a copy of the Manitoba Centre for Health Policy and Evaluation rules on "Preserving Confidentiality" as evidence of the extraordinary precautions taken to ensure confidentiality. Equally, she is of the view that it is rarely possible to know in advance the important research opportunities which data will present some 10 or 15 years later. As well, the Medical Research Council in their 1987 Guidelines on Research Involving Human Subjects recognized the importance of epidemiological research and emphasized the need to permit records research which does not require prior consent.

She is certain that while Canada should adopt guidelines which will protect the identity of individuals, they should focus on the preservation of the confidentiality of records and not deny researchers access to records for legitimate purposes. Such purposes will require that records be preserved for long periods of time and linkage across files be permitted. Care must be taken not to deprive society of the potential benefits which can flow from the conscientious use of data collected at public expense in the public interest.

Specific Proposals and Recommendations

The Advisory Council should take a different approach than the so-called European standards and any guidelines which the Council advances must recognize and preserve legitimate research opportunities.

Leslie L. Roos, PhD

Leslie Roos is the Director of the Manitoba Health Research Data Base at the Manitoba Centre for Health Policy and Evaluation, a Professor of Community Health Sciences in the Faculty of Medicine at the University of Manitoba, a National Research Scientist and an Associate of the Canadian Institute for Advanced Research.

As an active researcher involved in the analysis of large administrative databases for 19 years, Dr. Roos is not aware of any problems with their data. With appropriate confidentiality review of activities by university and government committees, the Manitoba health care data has been used for a number of individually-based longitudinal studies and privacy protection has been successful. He would be glad to share details of their privacy

protection measures with the Council and he also enclosed a copy of the 1993-94 Annual Report of the Manitoba Centre for Health Policy and Evaluation which contains details of research projects undertaken by the Centre.

Jorge Segovia, MD, MPH

Jorge Segovia is Professor of Social Medicine and Associate Dean of Community Medicine in the Faculty of Medicine, Health Sciences Centre at Memorial University of Newfoundland.

The development of large databases has resulted in significant improvement in the capacity of health researchers to design and construct important studies to monitor and evaluate the delivery of health care services and to study the outcomes of therapeutic and diagnostic procedures and drugs. For many years, research involving human subjects has been approved by ethics committees at the university or faculty level to ensure informed consent by participants and the preservation of confidentiality and anonymity. However, new advances in technology now permit the linking of several sources of data to the benefit of this research.

It is extremely important to achieve a proper balance between strict protection of the rights of individuals and the benefits of health care research. This requires a clear distinction between data obtained for business or commercial purposes and data for scientific research, as well as a constant review of ethical issues in research.

Evelyn Shapiro, MA

Evelyn Shapiro is a Professor of Community Health Sciences in the Faculty of Medicine at the University of Manitoba, a Member of the Faculty of the Manitoba Centre for Health Policy Evaluation and a past Chairperson of the Manitoba Health Services Commission.

As a health services researcher for over 20 years, Professor Shapiro has grave concerns about the importance of the Discussion Paper. She is confident that their system, getting prior approval from the province's Access and Confidentiality Committee and of the Faculty of Medicine Ethics Committee, and by using fake identifiers, has both protected privacy and produced studies from which federal and provincial governments have profited. She wishes to assure the Advisory Council that there never has been and she is confident that there never will be any breach of confidentiality in the use of health service data.

To do both cross-sectional and longitudinal studies which are critical to policy makers, file linkage is critical. Also, longitudinal studies, required to predict serious events and trends in service usage or the incidence of

specific diseases, cannot be carried out if time limits are placed on data storage. Furthermore, obtaining prior consent would make it impossible to produce the studies in the time frame required by decision makers and would be entail exorbitant costs. Adoption of the European model is especially worrisome because many researchers in Europe have found it impossible to continue doing longitudinal research.

She believes that population-based health services research is essential to policy making, and that there is a need to protect access to data while ensuring individual privacy.

Colin L. Soskolne, PhD, FACE

Colin Soskolne is a Professor of Public Health Services in the Faculty of Medicine at the University of Alberta. He is making a submission as the Chair of the International Society for Environmental Epidemiology's Standing Committee on Ethics and Philosophy and as a Member of the American College of Epidemiology's Ethics and Standards of Practice Committee.

He is concerned that Canada avoid the seriously negative position in the European Community which seems destined to render impotent epidemiology's ability to undertake health risks research. As evidence, he attaches copies of two letters to the European Community, one by the International Society for Pharmaco Epidemiology and the second by the International Society for Environmental Epidemiology. Both highlight the perennial ethical tension between the known public good that comes from epidemiology's linking of personal information and the potential for individual harm through access to personal information. He believes the latter concern to be only theoretical because there is no known case in Canada where researchers have compromised the privacy of records on which they have worked. To safeguard the public interest, epidemiology has developed ethics guidelines, including the need to maintain confidences and the privacy of data. Furthermore, for national and provincial linkages, oaths of secrecy are required for those who work with data.

He believes that the Discussion Paper has a distinct business bias (except for page 8, column 1), therefore he did not want public health arguments to go unattended. The self-interest of those trading in information must be distinguished from the public interest which is the concern of, among others, epidemiologists.

R. A. Spasoff, MD

Dr. Spasoff is a professor of epidemiology and community medicine in the Faculty of Medicine at the University of Ottawa.

He is concerned that, in worrying about the potential for abuse in commercial use of electronic data, we should not forget the benefits of using such data for health research. The proposals for protection of data in Canada, as well as those in the European Community draft directive, have the potential to stifle epidemiological research, thereby harming the health of the population. Issues of particular concern to epidemiologists are: retention of enough identifying information to allow record linkage; retention of data long enough to exceed the time it takes for chronic diseases to develop; and, ability to use files for purposes other than those for which they were originally collected. He describes an example of a study of Canadian veterans who had been exposed to radiation which cost $40,000. A similar study in the USA, for which file linkages were not available, cost US$7,000,000.

He is not aware of a single case in which the privacy of an individual has been comprised in epidemiological studies using record linkage. He poses the question "Are we inventing a cure for which there is no disease?".

University of Manitoba, Research and External Programs

The submission is made by Terrence P. Hogan as Vice-President, Research and External Programs.

Although the right of individuals to control information about themselves is a highly valued and legitimate principle in Canada, the Advisory Council should be aware that electronic information plays an increasingly valuable role in research. This research is carried out under protocols which ensure there are no threats to the confidentiality of data and no breach of ethics. There is no awareness of any instance in which the confidentiality of physician or patient information has been comprised, thus individuals' privacy can be protected while ensuring the ability to conduct and benefit from important research.

Specific Proposals and Recommendations

The Council is urged to ensure that the use of databases and linking of records in academic research is addressed in a balanced and considered fashion.

University of Ottawa, Human Rights Research and Education Centre

The submission is made by Professor Valerie Steeves, Senior Research Associate, Technology and Human Projects.

In general, the Centre favours legislation and regulation in concert with effective voluntary codes, technological solutions and education.

The information Highway is more than a roadway where commercial messages pass back and forth, it is an interactive exchange involving millions of people where ideas are exchanged. Therefore, it is imperative that development be consistent with cultural values. The rapid rate of technological change has made it difficult for governments to regulate development of and conduct on the network. Accordingly, it is the government's responsibility to create a set of principles to ensure development reflects human values necessary to secure quality of life. Hence, it must develop a definition of privacy which goes beyond mere confidentiality of personal information and encompasses concepts of human dignity and autonomy.

The government must develop a national policy that actively promotes openness, access and inclusiveness. As well, a national policy setting out ethical guidelines will balance private interests against the public value of open and inclusive communications. Moreover, the promotion of universal access must be a key component in order to avoid disenfranchising marginal sectors of the community.

Approaches

I. Regulatory mechanisms must be created, supported by legislation, where appropriate, that address the many types of relationships which will be formed over the highway.

   These regulatory mechanisms should provide that: personal information held by governments and the private sector should be subject to strict guidelines with administrative and judicial enforcement mechanisms; exchange of information between corporations should be restricted to guidelines similar to the CSA guidelines; personal communications between individuals should be private, including workplace communications, with judicial remedies; and, public discussions over the highway should be open and inclusive and subject to the least amount of regulation. In addition, a national standard must include the following provisions: relevance and consent to the collection of personal information, including that shared between government departments; voluntary codes must recognize the importance of informed consent, subject to equality of bargaining power and recourse provisions; there must be an independent watchdog body with the power to enforce its decisions but subject to judicial review.

II. Voluntary compliance, based on effective enforcement mechanisms, has a number of advantages over government regulation, such as sectoral input and the spreading of the costs of administration. However, voluntary regulation has led to uneven results in the past. The success of voluntary compliance with industry-wide codes will depend on the strength of the enforcement mechanism.

III. The development of universally available encryption mechanisms should be encouraged.

IV. Public education and the generation of public debate and discussion is required. The government should seek out strategic alliances with public and private sector stakeholders to ensure education about relevant issues is made available to the public at large. The Centre is in the process of developing a number of educational initiatives including: an annual university-wide, interdisciplinary course on human rights arising from communications technology; a series of seminars for corporations on issues relevant to the marketplace; development of an online library on privacy, human rights and the information highway. It also has developed the largest database of Canadian constitutional and human rights materials in the country which should be online in 1995.

Answers to Questions

1. The government must develop a national policy which recognizes the following privacy principles and rights:
   - to be free from unnecessary surveillance;
   - to control the disclosure and use of personal information;
   - to be free from unnecessary or unwanted intrusions of information or solicitations;
   - to participate freely in social, economic and political debate with reasonable and affordable access to the means of participation.

University of Waterloo, Office of Research

Because the Discussion Paper does not deal specifically with university researchers, there is concern that they might be grouped with telemarketers and businesses whose use of personal information is designed for profit making.

Statistics Canada information provides databases of extensive and valuable information and there is a danger that it will be lost to researchers. This has happened in Europe, where health research institutes in Sweden and Denmark are no longer able to operate, because European regulations have not defined the use of personal information differently for different purposes.

Specific Proposals and Recommendations

The Advisory Council is urged to hold public meetings and publicize the Discussion Paper which was received indirectly and too late to gather comments from the university community.

Norah Duck

Mrs. Duck's submission is in response to an article in the Toronto Star on October 15, 1994. Although she does not own a computer and does not intend to, she has a number of concerns about privacy issues based on her personal experience. She objects to unrestricted requests for her age and SIN during routine commercial transactions, e.g. supermarkets, hotels and banks. Other concerns include, development of consumer profiles without consent which may be sold to third parties, and the exchange of personal information held by the government with foreign governments, e.g. the agreement between Canada and the USA to exchange tax information.

She has little faith in new privacy legislation because unethical people and institutions will always find a way to circumvent it. Therefore, she believes that a massive program is needed to educate people on how to guard their privacy, e.g. when to give out personal information and when to question it.

Brian Fitzgibbon

Mr. Fitzgibbon's submission is in response to an article in the Toronto Star on October 15, 1994. After 30 years in the computer software industry, he is doubtful that use of computers and the information highway will ever become universal for those with low paying jobs and because of lack of interest.

He also responds to four questions posed in the Toronto Star article.

- *Could a system evolve that allows better privacy for the rich than the poor?*

  It is impossible to provide everyone with a level playing field because the poor will probably not want to own a computer or access the information highway.

- *Should E-Mail be treated as a private letter or as company property?*

  E-mail should be treated the same as any other company correspondence because there is no difference between E-mail and any other business letter.

- *Will the fast growing telecommuting phenomenon - companies allowing workers to stay home and do their job - be a means for employers to electronically spy into the home?*

  Permitting an employee to telecommute will only be effective in relatively rare situations. Generally, it will cause a drop in

productivity. Counting keystrokes and comparing them to productivity only works for data entry clerks.

- *Should individuals have total control of their personal and transactional information?*

  Total control is not an option for the user unless the gateway provides some way of encryption.

Harold Genz

The individual's privacy must be safeguarded in the information highway. Therefore, it must be a pre-condition when designing the system. When information about buying habits is requested on the telephone or on a computer, an automatic message should appear stating that it is private information and cannot be given out.

Khalid Saeed, Holaser

While conceding that it is difficult to keep electronic and magnetic data secure, Mr. Saeed suggests five principles:

- all electronic information, just like written information, should be marketed only with the written consent of the person or party concerned;
- a person may waive the privacy of his personal information but only in regard to the party with whom he is engaged in a transaction;
- data which is resident on a linked or non-linked computer is the property of the party owning it, whether or not it is sent by E-mail;
- a person should have total control over his/her personal and transactional information, subject only to legal requirements;
- electronic spying on an employee in the home is most repellant, therefore, measures of evaluation should be based on the material and services forwarded to the office.

J.C. Holst

J.C. Holst's submission is in response to an article in the Toronto Star on October 15, 1994. The Government of Canada should enact legislation which states the do's and don'ts on the invasion of the individual's privacy.

Jorg P. Kranz

Mr Kranz, who has 31 years of experience in data processing, deals with a number of issues related to privacy.

He is concerned that there is a proliferation of data banks in both the government and private sectors of which individuals may not be aware, and which are sometimes accessible to both sectors, e.g. insurance companies can access provincial driving records.

The best way to ensure only authorized access would be to set up a central government controlled repository where all information about an individual is stored, to which the individual would have sole right of access, the right to correct errors and the right to control release of information to third parties. Although having the disadvantage of adding another bureaucracy it would make it policeable. The minimum safeguard must be clear identification of all data banks, with copies of the personal information contained therein being provided to the relevant individual to permit verification, correction and ongoing updating.

E-mail and Voice-mail, as with paper mail, should be treated as a private letter and the employer should be denied access, other than with the consent of the employee.

Counting of keystrokes, timing of phone calls or wiring video cameras to the network should be considered an invasion of personal privacy.

Individuals must retain control of their personal and transactional information, other than for criminal investigations.

Steven Lotz

Mr Lotz provides advice on solutions to privacy issues that he believes are inexpensive to government, yet protect the rights of individuals. He believes that individuals have the right and responsibility to make their own choices, whether they relate to free association, property or privacy, and the government should not interfere. The function of government should be restricted to defence of the country, police forces for the protection of individuals and a court system to mediate disputes. This freedom of choice and association extends to whether to buy or not to buy, whether E-mail is private or not, whether a vendor may sell a personal profile or not, and whether monitoring by employers is to be permitted or not. The government needs to realize that people are capable of taking responsibility for their own lives. Therefore, breach of any agreements, freely made, should only be adjudicated by the courts according to Common Law. Application of these principles to the information highway is not new, only the technology

is new. If the government intervenes, individuals will only lose these rights of choice and free association. Therefore, increased legislation and regulation should not occur because it is not necessary.

D.B. Morrow

D.B. Morrow's submission is in response to an article in the Toronto Star on October 15, 1994.

Particular concern is expressed in regard to personal information collected, held and used by banks. The views expressed relate to banks having signed contracts with all card holders and borrowers containing "information clauses" which permit use of the SIN, credits checks, advertising, swapping lists, etc. More importantly, however, in the case of the Royal Bank, its "information clause" has now been unilaterally extended to certain depositors, i.e. RRSP holders, (a copy of the Royal Bank's revised Retirement Savings Plan Agreement is attached to the submission). The revised agreement indicates that there is no need to inform the bank of acceptance of the changes and it should merely be kept for the record. The "information clause", included in the Agreement, states that personal information, including the SIN, held or obtained by the bank may be used for many purposes not directly related to the RRSP investment transaction. Furthermore, the information may continue to be held and used after the depositor ceases to be a client or the Agreement is terminated. Thus, he claims that not only have most people in Canada already had their privacy and use of SIN rights removed by their banker but, if they want these various services, they have no option but to comply with these agreements.

Concern is also expressed that when a complaint (copy attached to the submission) was made to the Superintendent of Financial Institutions of Canada, not only was it indicated that there was no authority in matters of personal contracts but a copy of the complaint was sent to the Royal Bank without permission. The Bank has now responded that, because of complaints, changes are planned.

A final concern is that if banks get into the insurance business they will already have information, based on banking contracts, available to use however they want.

R.B. Oulton

R.B. Oulton makes two points in regard to privacy issues.

First, the onus on privacy should rest with the person/company who might sell it, e.g. telephone and cable companies, magazine distributors and charities should get permission to publish/sell information that they have obtained.

Second, companies whose business it is to know details about a person (banks, trust companies, credit reporting companies) should be obligated to, (a) advise individuals that information has been requested about them, and (b) send a copy of the information to the individual.

Richard D. Speers, DDS

Dr. Speers states that the oft repeated quote "information is power" should be recognized for what it really is - the insatiable desire to benefit from collated information on groups and individuals. He also raises detailed concerns about privacy invasions in four areas.

The SIN was originally instituted by the Government of Canada to properly identify participants in federally sponsored plans. He gives numerous examples of extension of its use far beyond what could be envisaged when it was instituted, because at that time, despite warnings, the government did not believe it was necessary to control its use. Even in cases where there have been requests to restrict its use, this has been skirted by the use of permission forms to circumvent the issue. As a common identifier, its use has allowed the simple collection of huge amount of data which suggests that retrieval and comparison are not only possible, but probable. By using alternate numbering systems, the automatic comparison and accumulation will be more difficult.

Improper disclosure of any information about a patient can lead to loss of medical accreditation by a practitioner. Patients expect complete confidentiality and privilege in regard to their relationship with health professionals, similar to lawyer/client privilege. In the wrong hands, unauthorized access to medical records and charts can be devastating, the recent actions of Evelyn Gigantes and David Nantes are cases in point. In no circumstances should third parties be able to access patient charts or records unless the patient specifically requests such release, and then only for complaint purposes, litigation, or for transfer to another health care provider. However, at the present time, there is no legislation that prevents a third party from demanding medical records of a potential employee or insurance applicant. Also, now that banks have the right to sell life insurance, he is not aware of any legislation that would prevent medical information given for life insurance purposes being used to decide whether to grant or call a loan. Nor is the federal government free from criticism. Access to medical and dental charts for audit purposes is now practiced by both Revenue Canada and Veterans Affairs Canada. With respect to medical information, government agencies, employers, bankers, and insurers must be limited in the data they can access in the first place. Identifiable medical records must also be secure. Another concern relates to the storage and transmission of medical information. The storage of

such information by Canadian life insurance companies in Boston, Massachusetts may lead to the inability to deal with improper usage in Canadian courts.

Trust companies and banks have amassed vast amounts of information that reveal spending patterns. This allows for target marketing which can leave many individuals, especially the aged and infirm, open to abusive or aggressive solicitations. Also, credit information is amassed in central agencies. Any person who accesses those files must be identified in the file by name, date and under whose authority the file is opened. An individual to whom the file relates should also have access to this information. Similarly, if fiscal agencies sell data and information, they should seek specific authority from the individual to do so. No retribution should occur for refusal to allow such information to be released. With respect to financial data, individuals must be aware of what information is presently stored, how it is being used and to whom it is being released. Also, individuals must have full access to their information and have control over its destiny.

Government agencies also have amassed vast amount of personal data. In the past hospitals and government agencies have sold mailing lists to private agencies for profit. The sale of licence plate information by the provincial government is a case in point. Revenue Canada has also made promises that no one has access to income tax data and information. However, provincial finance departments now have access to that information and policing authorities also want access during criminal investigations.

Strong legislation must be in place to define the extent to which this information is used, stored and managed. Problems associated with credit agencies must also be addressed in future legislation.

The electronic transmission of medical and dental information must be considered. The transmission of all sensitive data must be accomplished with the utmost security. This means that the data would have to be encrypted or sent along completely secure lines.

Specific Proposals and Recommendations

The use of the SIN, other than by federal agencies for whom the system was implemented, should be stopped.

J.S. Tate

Strong concern is expressed over the historical abuse of the use of the SIN. The 1964 legislation which created the SIN failed to provide any safeguards on its use for purposes other than those specifically allowed, and no punitive measures were provided for those who abused the system. This has continued despite serious concerns of the Privacy Commissioner and various parliamentary committees, as well as representations made to MPs and Attorneys General.

Experience over the past 30 years has shown conclusively that the preferred choice of various governments, namely voluntary codes for the private sector and moral suasion, has not worked. That experience should be a strong incentive to the Advisory Council to hold personal privacy protection as the prime and ultimate goal.

Individuals should have total control over their personal and transactional information.

Individuals and organizations who violate the rules should face heavy and meaningful criminal sanctions.

Canadian Cable Television Association (CCTA)

The Canadian Cable Television Association is a national organization representing 816 members, the majority of which provide cable television to more than seven million Canadian households.

In overall terms, the CCTA does not recommend legislation and regulation. Rather, it submits that voluntary codes and standards, technological solutions and consumer education can work jointly to provide effective privacy protection. Every effort should be made to pursue these approaches to the fullest extent. Measures taken by the CCTA, since 1991, to implement a cable industry-wide privacy code, are also described.

Conscious of privacy concerns, particularly in regard to the viewing habits of consumers, the cable industry adopted a model of self-regulation which is inherently different from the self-regulation models of the banking, direct-marketing, insurance and telecommunications sectors. In 1988, the industry established the Canadian Television Standards Foundation (CTSF) which is an independent body whose membership is made up of 90 cable companies licensed by the Canadian Radio-Television and Telecommunications Commission (CRTC). Membership is voluntary and is not restricted to members of the CCTA. The CTSF administers the Cable Television Customer Service Standards, adopted by the CCTA and approved by the CRTC in 1991, as well as other codes and commitments adopted by the CCTA. It adjudicates complaints related to alleged breaches of the Standards, codes, commitments and other aspects of cable service by its members. None of its findings are vetted by the industry and they are available to the public. The "Confidentiality and Security" provisions of the Standards are based on the principles of the Privacy Act and commit members to keep customers' information confidential "in a manner consistent with the goal of affording protection from invasion of privacy for all their customers". Specifically, member companies must: maintain all personal information pursuant to the Privacy Act; allow customers to inspect their records; upon request by customers, remove their names from mail and telephone solicitation lists; and, ensure that all employees provide photographic identification when entering customers' premises.

Approaches

I. The CCTA does not favour a legislative approach because it goes against the trend toward a deregulated business environment which characterizes the new global competitive marketplace. Moreover, legislation tends to be inflexible and is insensitive to the varying practices and technological sophistication of various industries and

sectors. Legislation can also lead to complacency that "the problem has taken care of itself" and, if it is too general, could lead to too much regulatory power being vested in the courts. Finally, any federal legislation would be limited only to those sectors over which the federal government has jurisdiction and therefore could not provide uniform protection and rights across Canada.

II. The CCTA favours voluntary codes and standards because they are more sector specific. They allow information handling practices to be reviewed from a business standpoint and provide better integration within the relevant sector as well as heightened awareness of privacy matters. Moreover, they are more flexible and adaptable to technological developments, leading to more regular review. In addition, they can be used as educational tools to inform consumers of their rights, and they may offer more effective, accessible and less costly redress of grievances.

The CCTA strongly supports the long-standing efforts of the Canadian Standards Association (CSA) to develop a" Model Code for the Protection of Personal Information". It has been represented on the CSA Technical Committee on Privacy by the CTSF in the development of the draft code. The goal of the CSA committee is to develop a user-friendly voluntary code which would balance trade interests and business needs with the consumer's inherent right to privacy. Therefore, the CCTA hopes that any new initiatives of the federal government will not create a disincentive to implement the CSA code according to industry specifications.

III. The CCTA believes there is great potential for technology to enhance the privacy of individuals. The cable industry is working on expanding and developing this potential. This is evidenced by the initiative of the UBI Consortium where a combination of technological designs and systems is being pursued to safeguard personal and transactional data.

IV. The CCTA agrees that consumers need information and education about their right to privacy, the risks posed by technology, and what they can do to retain and protect their privacy. The cable television industry is committed to use its extensive network to raise the awareness of consumers and to inform and educate them.

Specific Proposals and Recommendations

The CCTA recommends that the CCA draft privacy code be given a chance to work before legislation and government regulation are adopted or advocated.

Canadian Satellite Users Association (CSUA)

The Canadian Satellite Users Association represents the broadcast users of Telesat Canada's space facilities.

In summary, CSUA's position is that legislative rules are only required for the most sensitive data and for data collected by mandate. Industry-wide codes of conduct are best suited to the national deployment of protection for other personal data. Consumer education and the wide use of technological tools will ensure that individuals exercise the appropriate control over the use of their personal data. The definition of privacy, data collection techniques, the control and security of data, and the relevance of the CSA model privacy code are also discussed.

CSUA discusses in some detail the definition of privacy. Use of the word "interruption" is questioned in the first part of the definition of privacy given in the Discussion Paper, "the right to be left alone, free from intrusion or interruption". It is seen as adding nothing to the concept of privacy because its use suggests that all interruptions - whether welcomed or not - are invasions of one's privacy. Rather, it is submitted that the concept of "uninvited" is the key to any notion of privacy intrusion in today's society.

The members of CSUA are seen as being increasingly involved in transactional entertainment, education and other business services to the public. This involves sophisticated measurement techniques, involving the collection of personal data, to enable them to be responsive to their audiences as viewer choices rapidly expand. The end result will be new business opportunities and better service to the public. In doing this, members are sensitive to the public's concern over privacy issues.

Current data collection techniques, in four broad areas, are described in detail. First, audience measurement is typically collected for broadcasters by third parties without any known privacy problems and is anonymous when the broadcaster receives it. Future measurement will be by "people meters" whereby data will be collected by the broadcaster direct from the viewer. Second, the home shopping sector involves the direct collection of transactional data by which aggregate levels of demand can be established. Third, transactional entertainment services are now commencing with the introduction of "pay per view" which also involves direct collection of personal information. In the future, direct home satellite services will require an authorization centre to effect the transaction and this may be done by the use of smart cards which will contain the viewer's coordinates and credit information. Fourth, educational broadcasters are involved in distant learning services. Personal data is important in developing programs, ordering fulfilment material, allowing the student applicable course and inter-institutional transfer, and for marketing of courses. In the near future interactive services, such as opinion polling, referendum voting and advertising responses, will also collect personal information.

The personal information, such as transactional data, telephone numbers, addresses, viewers' choices, students' results, viewers' coordinates and credit information, collected by these various services will have value to advertisers and broadcasters, as well as to third parties. Most importantly, it will permit the broadcaster to develop services which best meet the viewers' demands.

In regard loss of privacy, citizens are seen as accepting this in many circumstances. Mandatory collection of personal information by governments, e.g. taxation and criminal records, is a case in point. This collection and dissemination is usually covered by legislation and regulation. However, citizens also accept the provision of personal data in many other types of transactions. This situation is different from mandatory collection, in that it is part of a transaction willingly entered into. Therefore CSUA believes that the key in these situations is control and security of data subsequent to the transaction.

The principles relating to the protection of personal data are also discussed, ranging from the OECD guidelines to the CSA draft model code. CSUA submits that the CSA code will form an excellent source of national principles because they are neutral to technology and specific sectors of the community. As such, they will be able to be used by any legislation or industry-wide codes in the development of specific codes of conduct.

Approaches

I. Government legislation and regulations have been required for highly sensitive and mandated personal information. CSUA submits that legislation in the area of government collected information is appropriate.

II. Industry-wide codes on privacy have many advantages over legislation. They do not require public funds, can cover country-wide applications thus avoiding a patchwork of provincial legislation, and are best dealt with on a sector basis by allowing more flexibility to change as the industry changes.

III. Technological developments are providing greater security for transactions and data storage through encryption and controlled access. Given a clear set of national privacy guidelines, organizations will be able to evaluate technology changes in the light of privacy protection requirements.

IV. There is less concern with privacy when individuals understand what is happening and the benefits associated with the collection of personal data. The proposed CSA guidelines will provide an opportunity to publicize personal rights and can be used by provincial and federal privacy commissioners in educating consumers.

Consortium UBI

Consortium UBI was formed in January, 1994 with the following members: Canada Post; The National Bank of Canada; Hydro-Québec; Loto-Québec; The Hearst Corporation; Le Groupe Vidéotron Ltée; Videoway Communications Inc. Its mission is to build the first interactive, bi-directional, multimedia communications highway and to provide access to it by at least 80% of Québec households with cable access.

Since its inception, the Consortium has taken a number of technological and organizational decisions to ensure that privacy rights will be respected. On the technological side, these include: the introduction of a smart card to ensure the identification and authenticity of users; encryption of all confidential data on the network; and, the fact that there will be no "client files" for users.

On the organizational side, the Consortium has retained the services of the University of Montreal's Centre de Recherche en Droit Public (Professor Pierre Trudel) to develop a moral code, including the protection of privacy. The code will take into account the characteristics and functionality of the system as well as the concerns of individuals and providers of services. The methodology is composed of three steps. The first involved the listing of moral issues in order to analyze areas of conflict that might arise in the environment of an information highway to the home. The second involved the identification of the groups, associations or public representatives who are concerned with the moral issues identified. Interviews were conducted with more than 50 groups and a report summarizing their concerns is currently being finalized. The third will involve the production of a moral code integrating all these issues, including methods for preventing and resolving disputes. Because the study is not yet complete, the Consortium believes that it is too soon for it to respond formally to the Discussion Paper.

Specific Proposals and Recommendations

The Consortium believes that the Information Highway Advisory Council would benefit from the results of its research, which, to its knowledge, is the only such professional study undertaken by parties interested in providing access to the information highway. It requests that it be allowed to present its findings to the Council after they are completed in mid-February, 1995.

Information Technology Association of Canada (ITAC)

The Information Technology Association of Canada represents members in all segments of the computer and telecommunications hardware, software, service and electronic content sectors. They account for 70 percent of the industry's revenues.

In summary, ITAC supports enactment of legislation guaranteeing to all reasonable and appropriate levels of privacy protection and information security, as well as clear avenues of legal redress. Beyond the legislated levels, it believes that industry and consumers should be left to regulate themselves through the marketplace of competing information services, featuring various levels of information security at a range of costs. It also sees technological solutions and education of both consumers and the commercial sector as playing an important role. A definition of privacy is provided, various concerns re privacy are detailed, and a major principle re privacy is defined.

ITAC lists five principles to guide its approach to public policy for the emerging information infrastructure. Its submission focuses on the fifth principle "Rigorous attention to privacy and information security issues through strong private sector codes and enforcement bodies".

Personal privacy is defined as an individual's control over access to his or her person and personal information. Discussion about the ownership of transactional information is likened to discussion about intellectual property.

The protection of personal privacy is seen as having become a significant issue in the development of policies for the information infrastructure. A 1992 survey by Ekos Research Associates found that 92 percent of all Canadians are at least moderately concerned about their privacy, with 81 percent being of the belief that computers are reducing the level of privacy. Furthermore, the potential for linking databases for new purposes was found to be the biggest single concern.

Control over access to and the use of transactional information is seen as a major concern. In this regard, many transactions using the information infrastructure leave a "data shadow". As new information services are introduced, more sophisticated forms of transactional information will emerge. Therefore, individuals may not know how their information is being used. A further concern, relating to intrusion, involves the use of electronic surveillance to monitor behaviour.

It is also noted that while individuals have always shared personal information with others, they have tended to view further sharing of the same information as an invasion of personal privacy. Nonetheless, in the end, control of such sharing rests on the degree of information security. However, the ability to add value to information, by compiling, packaging and analyzing it, benefits not just information companies, but also individual Canadians who use the new information services and who fill jobs in the information technology sector.

One of the main principles espoused by ITAC is that individuals should be free to determine the appropriate level of privacy in their lives. This will entail freedom to choose whether or not to connect to the information

infrastructure, to accept or reject services that may affect their level of privacy, and to be free to subscribe to, and be charged for, only those services they wish to receive. However, they should not suffer reduced levels of service because of their choice.

Approaches

I. ITAC supports enactment of legislation guaranteeing to all Canadians consistent rights to reasonable and appropriate levels of privacy protection and information security, and to avenues of legal redress. More specifically, it will welcome legislation banning products or services designed to compromise privacy or information security, such as the use of scanners to intercept private wireless communications. Moreover, it supports legislation limiting use of personal information by agencies and institutions in the public sector. This would include the use of personal information by government, and by institutions such as hospitals, schools and police forces. Disclosure of personal information to government agencies by companies in the private sector, without specific legal authority, as well as the sharing of information by the medical, legal and banking professions, should be similarly limited. In addition, governments may wish to provide for "whistle blowing" in legislation, including the sharing of personal information with law enforcement agencies when service providers believe that fraudulent or criminal activities are taking place. Finally, ITAC believes that there is a need for legislation that defines which party is responsible for the illegal sharing of information. It recommends that there be a principle of joint culpability so that both the "sending" and "receiving" parties will have a clear interest in respecting their obligations.

II. Beyond the levels set in legislation, ITAC believes that industry and consumers should regulate themselves through the marketplace of available information services. Sectoral codes should specifically address the security of personal information: when it may be collected, stored and compiled; when, with whom and for what purposes it may be shared; how ownership of the information is determined; and, whose permission must be obtained beforehand. In this regard, ITAC strongly supports the CSA efforts to develop a model privacy code through a technical committee on privacy which has strong consumer and industry representation. Based on the OECD guidelines, the model code sets out ten privacy principles (see Appendix B), and could be used as a standard against which voluntary codes could be reviewed. In addition, it should help to protect Canada's global competitiveness in the light of the proposed EC directives which will restrict the transfer of information to countries lacking strong privacy protection. Finally, ITAC will support rigorous enforcement of the CSA and sectoral codes through either sectoral bodies or an independent private sector agency.

III. Technological solutions also have a part to play, including encryption standards. ITAC believes that public input into the planning and initiation of information systems should be encouraged. Also, while a protracted review of privacy implications would not be desirable in most cases, introduction of new personal information systems should be accompanied by submission of a privacy impact assessment to an independent authority for comment and public display.

IV. The public should be educated to become aware of the value of personal information and the fundamental rights and concepts involved in protecting it. Moreover, Canadians should be aware of government legislation and industry codes that exist, as well as the additional privacy protection measures that are available from information service providers. Furthermore, the sharing of some kinds of personal information tends to become more acceptable when the underlying rationale and anticipated benefits are understood. As well, educational programs should be developed for the commercial sector, because many businesses need to be reminded that information security should be integral to every business decision. For example, all contracts should include confidentiality clauses and employees should be trained in the importance of protecting personal information.

Specific Proposals and Recommendations

ITAC offers its services in assisting in the development of privacy impact assessments, business security codes and policies, and a strong campaign to educate the public.

Mobility Canada

Mobility Canada represents companies which supply one million Canadians with wireless telephony services.

Mobility Canada's submission deals basically with privacy protection as it relates to radio-based telephone communications. It is committed to provide its customers with the privacy protection they require for wireless communications, and to the protection of customer confidential information.

Its position has always been that Canadians who use wireless telephony should be entitled to the same degree of privacy and protection as those who use wireline services. In the past, it has presented its views to the legislative committee during the hearings on Bill C-109, an act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunications Act. In addition it has made representations to Industry Canada that the importation, manufacture and sale of digital and analogue scanners, as well as unauthorized listening to cellular calls, be

made illegal. It supports the recent recommendation of the Advisory Council that scanners and unauthorized interception of radio-based telephone communications be made illegal.

In regard to the protection of customer confidential information held by its member companies, it has already begun the adoption of a Code of Fair Information Practices which goes beyond the regulations currently imposed by the CRTC.

In addition, member companies of Mobility Canada actively educate their customers on privacy protection measures for cellular telephones. As well, they are committed to the provision of digital service which is more difficult to intercept and which enables the provision of high quality encryption at reasonable prices.

Radio Advisory Board of Canada

The Board believes that individual privacy is of paramount importance to Canadians and supports government/industry initiatives in strengthening privacy measures.

Its submission deals basically with privacy in radio-based communications. In its response to the 1993 "Public Discussion Paper on Radio Based Telephone Communications and Privacy", it recommended that all radio-based telephone communications be afforded the same level of privacy protection as is available on the un-encrypted wireline service. More specifically, it recommended a ban on both digital and analogue scanners and that the ban should encompass not only cellular frequencies but also other frequencies involved in private radio communications. These recommendations have been generally accepted by the Advisory Council and the Board urges speedy adoption.

RadioComm Association of Canada (RAC)

The RadioComm Association of Canada represents the wireless telecommunications industry in Canada including cellular telephone companies, public cordless telephone licensees, radio paging and mobile radio operations.

In general, RAC believes that all of the approaches set out in the Discussion Paper, involving industry/government partnerships, are part of the solution. It supports a strengthening of privacy protection measures in both the public and private sectors. Also, it deals specifically with radio-based privacy issues.

In regard to privacy issues, it believes that such concerns related to the information highway are well founded, particularly because of the increase

in personal information databases, including transactional databases, coupled with personal profiling.

Issues related to radio-based privacy also are specifically dealt with. RAC has commented on these issues in the past and fully supports the telecommunications privacy principles issued by the then Department of Communication in 1992, because it believes that Canadians have the right to the same level of privacy on radio-based communications as for wireline systems. Therefore, it supports the recent recommendations of the Advisory Council that existing legislation should be amended to make it an offence to intercept any radio-based telephone communications and that, in general, the manufacture, importation, sale and distribution of scanners capable of monitoring radio-based telephones be prohibited. It is concerned that failure to do so will hamper the deployment and evolution of radio-based telephony and Canada's role as a leader in this area could quickly erode.

Approaches

I. Other than for the introduction of legislation to curb the interception of communications, the Association believes that, although desirable, the adoption of a national privacy standards framework in all spheres of activity would be difficult because of differing federal/provincial jurisdictions.

II. RAC strongly supports the development of industry codes to deal with privacy matters. They can be strictly enforced through peer pressure and, in some cases, by the threat of sanctions from regulatory bodies. In this regard, RAC is developing an industry privacy code for its members, whether regulated by the CRTC or not, which would address the issue of confidentiality of customer information.

III. As technology develops, it becomes increasingly possible to provide privacy protection through technological solutions. For example, the wireless industry is rapidly converting to a system of digital transmission which is a more inherently secure form of transmission and allows for the use of digital encryption. However, RAC cautions that existing laws restrict the import/export of highly encryptable devices and that a common U.S./Canada encryption standard could be extremely difficult to achieve. Moreover, it cautions that, although technological sophistication can provide a more secure environment, it can also open up new avenues for abuse.

IV. RAC agrees that there is a fundamental and continuing need to educate consumers about privacy issues and states that the wireless industry is committed to provide privacy related information to their customers on a regular basis.

Specific Proposals and Recommendations

Regulatory and legislative measures should be brought into effect, without delay, to deal with the interception of radio-based private communications and a ban on scanners.

Rogers Cantel Inc.

Cantel operates a number of nationwide radiocommunications services, including cellular, paging and mobile data. It is also licensed to provide public air-to-ground telephone and cordless telephone services.

Cantel deals mainly with issues that pertain to its business and, in doing so, supports the submissions made by Rogers Communications Inc., the Information Technology Association of Canada, RadioComm Association of Canada and the Radio Advisory Board of Canada.

In general, it believes that the private sector should regulate itself and it is in favour of voluntary codes of ethics for the telecommunications sector, coupled with technological solutions and consumer education. If, however, because of the voluntary nature of codes, some participants seek to avoid their terms, the federal government should take all necessary steps to ensure that all participants are under the same commitment regarding information privacy. General privacy principles and the privacy of radio-based services also are dealt with.

Privacy of customer information and communications is an important issue for Cantel.

On the issue of general privacy principles, it believes that, to ensure wide use of the new and innovative services that the information highway promises, people will have to be provided with their desired level of information and communications privacy.

In regard to the privacy of messages carried over wireless communications devices, Cantel believes that Canadians should enjoy the same level of privacy protection in wireless communications and information highway services as is guaranteed in the Telecommunications Act for wired communications. It also points to the number of well publicized cases which have brought to the forefront the ease with which cellular transmissions can be intercepted. Accordingly, it supports the recent recommendations of the Advisory Council that existing legislation should be amended to make it an offence to intercept any radio-based telephone communications and that, in general, the manufacture, importation, sale and distribution of scanners capable of monitoring radio-based telephones should be prohibited.

Cantel believes that in order to ensure the privacy of Canadians, through the end of this century and beyond, the following privacy principles should be adhered to.

Individuals should have control over the use of their personal information and have a choice in the desired level of privacy.

All data and voice messages originating on any personal communications device, whether wired or wireless, should be deemed private, and intentional interception and/or disclosure of said information should be a criminal offence.

Beyond the basic protection outlined above, government and industry should ensure that Canadians are fully aware of their choices and should be free to choose their desired level of privacy.

Approaches

II. Cantel supports a universal code of ethics for the telecommunications industry which could be modelled on the draft CSA model code. Similar codes are already in use in various sectors of the industry, some of which have been mandated by CRTC decisions. Therefore, Cantel submits that all participants should be required to conform to the same code, regardless of whether or not they are regulated by the CRTC, thereby ensuring a level playing field. Furthermore, it believes that failure by the Minister to use all the means at his disposal to ensure that the privacy protection provision of the Canadian Telecommunications Policy, as enshrined in the Telecommunications Act, will create competitive distortions and will negate much of the protection sought by Canadians. Finally, it sets out that portion of its Terms of Service which deals with confidentiality of customer information covering consent to disclosure and inspection of records.

III. Two aspects of wireless communications technology can alleviate the problems of unauthorized interception. Digital service is now available to 75 percent of Canadians and is not intelligible to analogue scanners. Digital scanners are not yet available on the Canadian market. Moreover, encryption services should be available on digital services early in 1996. Therefore, although digital technology is inherently more private, Cantel submits that the federal government should take immediate measures to preserve this privacy until encryption services become available.

IV. Education of users is a responsibility of both government and industry because it is extremely important to spread awareness of the choices available to customers in order to ensure their desired level of privacy. For its part, Cantel distributed a circular on the safe

use of cellular phones, as a bill insert, and provides customers with the relevant sections of its Terms of Service relating to confidentiality of customer information.

Specific Proposals and Recommendations

Adoption of an industry-wide privacy code should become a condition of the granting of a wireless communications service provider's licence.

Rogers Communications Inc.

Rogers Communications is a diversified Canadian communications company with interests in cable television, broadcasting and telecommunications.

Rogers comments are also provided on behalf of its subsidiaries and associated companies, including Rogers Cablesystems and the Canadian Home Shopping Network. As well, it fully supports the submissions made by Rogers Cantel and Unitel.

In summary, Rogers believes that effective voluntary codes supported by appropriate technological safeguards and consumer education are clearly the best approach. It sees additional legislation or regulation as an inappropriate choice. It also sees the critical issue facing the Advisory Council as being how to protect privacy without comprising the benefits of the information highway. A number of concerns are expressed which should be taken into account when dealing with the critical issue.

Rogers agrees that the public is concerned about the security and privacy of sensitive personal information on the information highway. However, in dealing with the critical issue, Rogers has other concerns that should be taken into account when developing privacy measures.

The information highway is evolving and dynamic, and the pace of change is rapid. Therefore, privacy measures must be compatible with this dynamic and often unpredictable evolution of the highway.

Measures to protect privacy must be capable of general application to all networks and service providers in a competitive environment. Therefore, in seeking a competitive environment, Rogers submits that a corporation which provides services through subsidiary companies should not face restrictions on the use of personal information that are not faced by a corporation which provides services through an integrated organization made up of a number of divisions. The same privacy rules should apply to both organizations with respect to the transfer of personal information to market services and to evaluate credit risk.

In the complex and constantly changing environment, network providers cannot effectively police privacy. The problems of telephone companies in trying to police telemarketers highlights this problem. Therefore, privacy measures must focus on information providers, and network providers should concentrate on technical safeguards and consumer education.

Now that speech, text, images, sounds and moving pictures can be combined, transformed and transmitted as digital signals, the potential for loss of intellectual property rights becomes a much greater problem. Accordingly, privacy protection measures must be balanced with the rights of creators to know who is using their intellectual property.

Approaches

I. Rogers believes that additional legislation and regulation would cause too many problems. Legislation is a blunt instrument which cannot effectively respond to the rapidly changing environment of the information highway. In addition, a legislative approach would require complementary federal and provincial legislation in order to ensure equal treatment of competing businesses and of consumers. This would require too much time and effort, as well as the requirement for additional public sector resources.

II. Effective voluntary codes overcome the disadvantages of legislation, particularly because they are more flexible in meeting the needs of customers, the marketplace and the regulatory environment of the industry. In order to promote the credibility and relevancy of voluntary codes to all information highway players, Rogers strongly supports the CSA initiative to develop a model privacy code as a standard. Based on the OECD Guidelines, the CSA code is being developed by a committee comprising a broad range of interest groups representing consumers, business, labour and government. It will also provide a standard by which the international community can measure the effectiveness of Canada's protection of personal information.

III. Rogers supports the use of technology, including encryption, to protect personal information on the information highway. It also believes that consumers can become involved in the technology development process by the participation of consumer groups in the development of CSA technical standards, for which CSA provides funding.

IV. The need for consumer education on the protection of personal information is also endorsed. Such education must be a shared responsibility between individuals, governments and businesses. Also, the publishing of the CSA standards should assist in this process.

Stentor Telecom Policy Inc.

In overall terms, Stentor does not support additional privacy legislation at this time but submits that a combination of a strong national voluntary code, technology solutions and public education is the right mix of privacy protection for the information highway. If, over a reasonable period of time, this combination proves inadequate, harmonized national/provincial legislation should be considered as the next approach, building on the privacy principles, the technology solutions and the practical experience gained through voluntary self-regulation. A background is provided as to how Stentor companies have and are approaching privacy issues. Consumer privacy concerns are reviewed in detail. A comprehensive description is given of present and future developments and services on the information highway. Also, detailed comments are made on specific privacy issues relating to: transactional data and personal profiling; transactional security and individual identification; monitoring and surveillance; and, intrusion.

From the earliest days of telephone service, protection of privacy has been an underlying principle of the Canadian telecommunications system. Stentor companies also have recognized a responsibility to protect customers from intrusions, such as indecent or harassing calls, and are continually introducing new services that allow customers to establish their own level of privacy protection. As well, Stentor is committed to achieving the objectives of the Canadian government of creating jobs through innovation and investment, reinforcing Canadian sovereignty and cultural identity, and ensuring universal access to the information highway at reasonable cost. It also is committed to the principle that the highway should provide a level of privacy protection and network security that satisfies the privacy of Canadians without limiting its other benefits.

The information highway is seen as a national broadband communications system carrying voice, text, data, graphics and video services to and from virtually all Canadians through a network of networks owned and operated by different service providers. Detailed examples are provided of developments now underway such as: the Beacon Initiative of the Stentor companies to provide interactive broadband access to between 80-90 percent of all homes and businesses within ten years; medical and educational linkages in many provinces; etc. Rather than the so-called 500 channel universe, the information highway will facilitate creation of a "personal channel" that reflects the specific interests and needs of each user.

The most relevant studies indicate that the use of personal information and the right to be left alone are the key privacy issues on the emerging information highway. Changes on the highway are also bringing about an unprecedented emphasis on privacy issues and, as the technologies develop, new ways to address privacy. The benefits of future investments

in information highway infrastructure and services will be greatly diminished unless Canadians feel comfortable with the level of privacy protection that the networks afford.

That Canadians are concerned with privacy issues has been reflected in several surveys conducted in recent years, particularly the Ekos Research Associates survey of 1992. The Ekos study leads to the conclusion that while Canadians are concerned about controlling their personal information, there is more acceptance of its use in specific situations where the purpose and benefits are clearly identified. Furthermore, when a business relationship has been established, further use of customer information within an organization is less of an issue. Under the right to be left alone, the Ekos survey indicates that telemarketing is seen as more of an annoyance than ad mail or door-to-door selling. Also, it is pointed out that Canadians have taken measures to protect their own privacy. While being very concerned with privacy, it is believed that Canadians do not wish to forego the benefits that have resulted from computer and communications technology. What seems to be required is a balance between reasonable and unreasonable uses of personal information and adequate means to allow individuals to set limits on how their information will be used.

In terms of freedom from intrusion, many examples are cited of monitoring and surveillance and intrusion. A typical example of monitoring and surveillance is the "electronic leash" created by the enhanced tracking capabilities inherent in wireless or satellite-based personal communications systems whereby, in the absence of effective controls, the actual location and movements of an individual can be tracked in an unauthorized manner. Employee monitoring, whether by video surveillance or electronic productivity monitoring, is also seen as a significant concern. Surveillance of E-mail, whether by employers or outside sources, is also a concern, as is the use of scanners to intercept cellular or other radio-based private communications. Finally, surveillance at home is seen as a potential problem in the light of proposed systems which will allow the provision of security services by electronic means, electronic monitoring of consumption and service by utility companies, and interactive multimedia services on TV and home computer systems. Nevertheless, surveillance and monitoring are not seen as totally negative. Their significant benefits are recognized in the fields of home security, search and rescue, commercial fleet management, etc. It is all a question of the uses to which monitoring and surveillance are put. Intrusion is also seen as a concern. This may take a variety of forms but the most common concerns relate to telemarketing. However, the impact of telemarketing has been alleviated, to some degree, by recent CRTC decisions which have restricted the use of ADADs.

Detailed comments also are made about concerns about protection of personal information. These include transactional data and personal profiling, and transactional security and individual identification. Many examples are given which indicate that while there can be important

negative aspects to these issues, significant benefits can also accrue, provided that adequate privacy controls prevent the unauthorized use of personal information and that consumers have rapid and easy access to limitations on its use. Consent to use or transfer of personal information is also seen as a key aspect. However, Stentor believes that imposing such a requirement without a phase-in period would cause significant economic upheaval within Canada's direct marketing industry.

Answers to Questions

1. Privacy protection revolves around three issues: the need for fair information practices to establish ground rules for the use of personal information; the right to be left alone; and, the necessity for information service providers, technology developers and users to be sensitive to broad consumer privacy concerns. On the first issue, Stentor believes that the ten principles within the CSA model privacy code, which interprets the OECD guidelines in the Canadian context, provides a cohesive and comprehensive basis for personal information protection on the information highway. Stentor used the OECD guidelines in the development of its own "Model Code of Fair Information Practices" which governs company practices with regard to the collection, storage, protection, use, disclosure, individual verification, and correction of personal information. On the second issue, the right to be left alone (one of the six "Telecommunications Privacy Principles enunciated by former Minister of Communications Perrin Beatty) must be incorporated as a principle in the development of the information highway. In regard to the third issue, Stentor believes consumers should have maximum choice in matters of telecommunications and information highway privacy and the choice of privacy level should not limit access to network services and information.

2. Stentor companies believe it is premature to introduce broad or sweeping legislation or regulations. A fundamental principle of lawmaking should be to enact legislation only when other measures have failed to work. Therefore, the government has the opportunity down the road to introduce privacy legislation if voluntary codes, coupled with technological solutions and consumer education, fail to protect individual privacy. Also, early privacy legislation or regulation that does not reflect market realities may hamper or dissuade information highway investment. Furthermore, any eventual legislation should be structured to reflect and respect the principles of any successful industry codes.

3. Stentor sees the information highway as a national inter-operable network of networks with interactive multimedia services being provided at the local, regional, provincial, national and international levels. Therefore, a national approach to privacy protection is

needed to address cross-border services and in order to avoid consumer confusion due to differing levels of privacy protection in various regions of Canada. Provincial or sectoral legislation will only lead to increasing "balkanization" of privacy, and would create false economic incentives for business to establish in those regions with less stringent requirements. Although Stentor would not be fundamentally opposed to legislation on a national basis in order to ensure a level playing field across Canada, it is concerned about the lengthy effort required to harmonize federal/provincial legislation. Thus, a national approach of voluntary self-regulation is preferred in order to ensure early national coverage and protection. The extension of the federal Privacy Act to federally regulated institutions is opposed because of its complex and burdensome administrative processes, because the CRTC has clearly mandated responsibilities in regard to privacy protection, and because many of the information highway service providers are not federally regulated, therefore a level playing field could not be ensured.

4. Stentor believes that the most effective role for the federal and provincial governments to play at this time is to monitor the development and application of voluntary principles within the private sector while, at the same time, overseeing the protection of personal information in new interactive services developed jointly by government and the private sector. It endorses the development of a national voluntary code for personal information protection. Such a code will provide all information highway users with a set of privacy principles with which to establish common privacy ground rules. The reputation of companies developing new information highway services, the power of consumer choice, strong internal controls, and the market risk inherent in failing to adequately address privacy concerns are all powerful inducements for companies to develop and maintain effective privacy standards. Stentor supports the introduction of a national voluntary code for the protection of personal information and actively supports the efforts of the Canadian Standards Association (CSA) to develop and implement such a code.

5. Personal privacy will be enhanced by new software and hardware solutions which will enable most users to reasonably and cost-efficiently achieve the privacy protection level of their choosing. However, privacy protection is not the only criterion for the design of future interactive services. Innovation and the cost of the services may be impeded if the information highway standards, particularly for data security, are excessively stringent or established without regard to the various applications on the highway. The design of future information highway services should enable individuals, perhaps by the establishment of separate "tiers" of information highway use, to

determine and achieve the level of privacy protection they require. For example, access to on-line medical records and banking applications will require sophisticated privacy protection features while the Internet will provide little more than the availability of encryption, if required.

6. Canadians can exert considerable influence on the design process of new technologies through a variety of means, including consumer and public advocacy groups, public proceedings for regulated service providers, use of the media, contacting service providers directly and, when new services do enter the marketplace, by "voting with their feet". The exercise of consumer choice has become a powerful marketplace force, therefore, without adequate consumer trust, applications development on the information highway will be an extremely risky prospect. Accordingly, information providers will be extremely conscious of privacy concerns.

7. Consumer education is an essential element in the future success of the information highway. The Stentor companies believe both government and business have an obligation to inform and educate Canadians about privacy protection. All Stentor companies are actively involved in informing their customers of their options for protecting privacy and will be collaborating with other organizations in the implementation of the CSA code, as well as the significant public education efforts required to promote its use and relevance to consumers.

TELUS

TELUS is the publicly traded management holding company of AGT Limited and AGT Mobility Inc. which provides telecommunications services and wireless services throughout Alberta.

In summary, TELUS does not believe that additional legislation and regulation is required. In its view, self-regulation, supported by industry promoted education and technological solutions, is the most effective answer to the public's privacy concerns. In addition, it reviews public concerns, the history of its own self-regulation efforts, and the role of the CRTC in ensuring adequate privacy protection.

TELUS believes that Canadians recognize the potential of the information highway in terms of the choice of services and service providers it will bring. This is evidenced by the high percentage of positive responses received in the TELUS Longwoods Survey of 1994 and the Gallup Poll of 1994. However, both of these surveys found that an equally high percentage of respondents were either very to somewhat concerned about privacy on the information highway or were concerned about appearing on mailing lists,

and about the wrong people gathering financial and other personal information about them. In the Longwoods Survey 39 percent of respondents felt that their privacy concerns were so high that they would probably not use the information highway. TELUS believes that many of these concerns relate to future privacy issues which might emerge as the multimedia services and complex technology of the highway evolve. However, it concludes that their must be a balance between the development of new services and public privacy concerns, if the full benefits of the highway are to be realized.

The effectiveness of the telecommunications industry's privacy protection initiatives, particularly those of TELUS, are reviewed in detail. AGT was the first telecommunications company in Canada to introduce "Call Display" and Call Management Services. Before doing so, it consulted with women's shelters, social services, law enforcement agencies, medical professionals and other groups. As a result, various privacy protection features, related to call blocking, call trace, and deactivated call return, were introduced. In addition, AGT has adopted a Code of Fair Information Practices based on the Stentor model code. This code addresses the collection, retention, access to, and use and disposal of personal information, as well as security safeguards and accountability and openness. The code applies to both customers and employees. All of these initiatives have been well received by the public and are seen as evidence of how well self-regulation can operate. In this regard, AGT is actively involved in the development of the CSA model privacy code.

The existing powers of the CRTC, based on the provisions of the Telecommunications Act, for the enforcement of privacy provisions in the telecommunications industry are also reviewed in detail. These provisions have been used by the CRTC to impose self-regulatory privacy standards on the telecommunications industry, as well as to regulate unsolicited telecommunications.

TELUS sets out a number of principles that guide AGT in its development and offering of new services which are as follows.

- Privacy-sensitive customers should be offered service options that allow them to best manage their own privacy requirements.
- A called party has the right to know who is calling them, even without answering the phone.
- A calling party has the right to protect their anonymity, especially if potential risk or harm is involved.
- All called parties have the right to defend themselves against anonymous, especially harassing calls.

- All customers have the right to be informed in advance, in plain language, of the privacy impact of any new service, including protective measures.
- When customers' privacy interests change, by virtue of a new service, they must be given the opportunity to mitigate, as much as possible, adverse privacy consequences at no extra charge.

Although TELUS is aware of the strong demand for the legislative option, it is of the opinion that the need for legislation has not been demonstrated and therefore legislation is not needed. It submits that self-regulation will continue to be the most effective way to address present and future privacy concerns. Legislation would cut service providers off from essential direct customer interface and would impose additional government agencies and time-consuming review processes.

TELUS believes that self-regulation and the use of voluntary industry codes will be the most appropriate and effective way to ensure that privacy concerns are met in the most cost-effective and customer focused manner. CRTC, with its support for voluntary codes, has sufficient authority to regulate on privacy issues in the telecommunications industry. As well, addressing privacy concerns has become an integral part of service offerings. Therefore customers will have the choice between varying services and service providers, and competition will weed out unresponsive enterprises. Moreover, self-regulation allows quicker response to new issues.

In-house education is vigorously pursued by TELUS. Copies of its code and an information brochure have been distributed to its employees. Information sessions are held, and a video has been developed in order to ensure that they are aware of their privacy rights and the rights of customers.

Answers to Questions

1. TELUS supports a privacy regime characterized by the following features:
   - reliance by service providers on voluntary codes such as those of Stentor and CSA;
   - scrutiny by the CRTC and willingness to use its powers to ensure that service providers meet their privacy responsibilities;
   - increased public education by the federal government, the CRTC and industry; and,
   - increased commitment by industry to ensure that technological and customer-focused solutions to privacy concerns keep pace with new service developments and privacy issues.

2. There is no demonstrated need to introduce additional legislation. The federal government and the CRTC should support voluntary codes of conduct which would be supplemented by education and technological developments.

3. All domestic means of accessing the information highway are currently subject to federal regulatory jurisdiction. Therefore, this is sufficient to ensure a consistent national level of privacy protection for users of the highway.

4. Voluntary privacy codes, augmented by existing regulatory mechanisms, will continue to be the most appropriate means for privacy concerns to be responsibly addressed. The importance of existing deterrents to privacy violations in the Criminal Code and consumer protection legislation should not be overlooked.

5. Successful service providers on the information highway will have very powerful incentives to ensure that their service offerings meet the privacy needs of their customers.

6. In the competitive information highway environment, the purchasing behaviour and service preferences of consumers will signal to service providers whether they are meeting privacy needs. Moreover, market surveys, focus groups and service trials, prior to full commercial introduction, will ensure that privacy demands of the market are met.

7. Responsible companies can make sure that customers are aware of their privacy rights and the obligations of companies with respect to the use and protection of personal information. Government can also complement this through existing consumer awareness activities of Industry Canada and provincial departments of consumer affairs.

Unitel Communications Inc.

Unitel concurs in the submissions made by Rogers Cantel Inc. and Rogers Communications Inc.

In summary it is of the opinion that there is no need to introduce additional legislative and regulatory measures, other than those which already exist. Rather, it believes that voluntary codes supported by technical solutions and consumer education are the most effective means of protecting consumer and employee privacy. Unitel also believes that Canadians are genuinely concerned with the potential erosion of their personal privacy in the information age. In addressing the questions asked in the Discussion Paper, it outlines the various measures that it is taking to address the privacy concerns of its customers and employees.

Answers to Questions

1. In Unitel's view, the six Telecommunications Privacy Principles, adopted by the then Minister of Communications in November 1992, should serve as the basis of an effective privacy protection policy for consumers of telecommunications services. Moreover, they will assist service providers to develop their own policies and procedures. Unitel is currently modifying its own code based on the Principles and on the principles set out in the CSA's draft Model Code.

2. Unitel submits that, in so far as regulated telecommunications carriers are concerned, stronger privacy protection measures are not necessary to date. They could undermine the efforts of the CSA to develop its model code which has widespread support from consumer groups, government and industry. The introduction of competition within the industry has forced it to become more sensitive to the privacy concerns of its customers and this is an important factor in the retention of customers. Also, regulated carriers are bound by the confidentiality provisions of their Terms of Service (a copy of Unitel's Article 11 of its Terms of Service which includes use, disclosure and inspection provisions is provided in its submission). Moreover, regulated carriers are bound by the privacy provisions contained in section 7(i) of the Telecommunications Act and section 41 of the Act which permit the CRTC to regulate unsolicited telecommunications. In this regard, the Commission has already taken action on restricting the use of Automatic Dialing-Announcing Devices (ADADs), limiting the use of junk facsimiles and live voice calls for solicitation purposes, and directing the provision of free per-call blocking of name display on a universal basis. Finally, in 1994 the Commission ruled that it would not grant speedy approval to the competitive filings of telephone companies if those filings raised privacy concerns.

3. For the reasons set out in the answers to question 2., Unitel is of the view that additional federal, provincial or sectoral legislation for regulated telecommunications carriers is unnecessary. In addition, the vast majority of regulated carriers are active participants in and fully support the development of the CSA model privacy code.

4. It strongly supports voluntary codes which will allow businesses to customize privacy policies and procedures in a manner that is appropriate to the nature of their business and clients. Therefore, it is participating in the development by the CSA of its model code. This code, based on the OECD Guidelines, will be used by businesses to develop their own codes which, in turn, will be submitted to the CSA for approval. It notes that the Privacy Commissioner has been particularly supportive of the CSA initiative.

Moreover, voluntary codes are more flexible than legislation and can be easily adapted to changes in the privacy expectations of consumers over time, a potential event which was recognized in the government's Telecommunications Privacy Principles.

5. Unitel agrees that it is not technology itself that may threaten privacy but the uses of such technology. It believes that technology should be used to maximize privacy, such as the provision of free per-call blocking in relation to call display features. Furthermore, because of the statutory requirement that carriers not interfere with the content of customers' messages, they should not and cannot be expected to play the role of "traffic cop" on the information highway. It is information providers and not carriers who should be responsible for privacy violations when they are clearly responsible.

6. Unitel notes that, as far as regulated telecommunications services are concerned, a forum already exists where consumers can make their views known about new technologies and services and how they may impact on personal privacy. This takes the form of public hearings of the CRTC. In addition, consumers will be able to submit comments to the CSA on its draft model privacy code. Unitel expects, that once the code has been formally adopted, the CSA will continue as a public forum for the discussion of privacy issues.

7. Educating consumers about privacy is clearly in the public interest. Both government and business have a role to play. Also, by making their concerns known, consumers can also share in this responsibility.

Specific Proposals and Recommendations

Unitel submits that if additional privacy protection measures are adopted as a result the Advisory Council's proceedings, there are legitimate reasons, as outlined in its submission, why the regulated telecommunications sector should be exempt from the application of such new measures.

Association des consommateurs du Québec Inc.

In summary, the Association concludes that the various levels of government should enact legislation to ensure that privacy and confidentially of personal information is respected, and that only the minimum amount of information, necessary to uniquely identify an individual, be collected.

The Association notes the explosive nature of computer technology and the journalistic hype which has surrounded the development of the information highway. Only recently have governments reacted by creating committees and commissions to study its effects and fallout, including respect for privacy. The Association identifies three factors that contribute to the urgent need for legislation: private sector initiatives such as the UBI Consortium and Bell Canada's Sirius project demonstrate that consumer access to the electronic highway is not far off; the quasi-exponential growth in the amount and variety of information services; and, the differences in legal and judicial systems in the various jurisdictions within Canada, coupled with the proverbial lethargy with which the legislative bodies study and then enact new legislation. Given the impact of the three preceding factors, the Association strongly recommends that the various levels of government give priority to the issue of privacy on the information highway

In responding to the question posed on page 17 of the Discussion Paper, "Is it a responsibility of government, or should it be up to the marketplace to determine what levels of privacy protection will be offered?", the Association makes it clear that it cannot imagine industry ever voluntarily limiting its hunger for consumer information. Furthermore, it believes that elected representatives ought to put the concerns of their constituents in first place, given the enormous resources which can be brought to bear by industry. Therefore, governments ought to assume vigourous leadership to counteract privacy intrusion.

The Association then addresses the next question on page 17, "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?". A minimum level of privacy must be assured to all Canadians, regardless of income or social status. While it is foreseeable that certain services will entail cost for providing a level of privacy protection which is more stringent than the minimum level, the cost of providing a minimal level of privacy protection must be absorbed by industry.

Finally, the Association deals with the question of confidentiality. The key to the whole issue lies in defining the point at which the use of information about a specific consumer becomes excessive. A certain amount of personal information is required by institutions who deal with the public on a

regular basis, and this can involve more than simply the name, address and social insurance number of the individual. The following questions should serve as a guide in determining whether an abuse has or could possibly take place: has the institution collected significantly more information than is necessary for the completion of the task at hand, or has the institution not been authorized by the individual, or by Canadians as a whole, to collect the information?; can the information be accessed in such a way that one individual can gather personal information about another?; can the information be accessed by institutions and/or marketing specialists to further target or influence potential clients?

Colin J. Bennett

Colin Bennett is a well known and much published privacy advocate. He is an Associate Professor in the Department of Political Science at the University of Victoria.

In summary he believes that there is widespread agreement on the principles of fair information practice; nobody wants to be seen to be against the privacy of the individual, nor to belittle the genuine fears of the Canadian public. Therefore, the regulatory status quo is not an option and we need to apply the full range of policy options to the problem, self-regulatory codes, legislation, privacy-friendly technologies (encryption) and consumer education. None of these options is sufficient by itself. He also provides a summary of the development of privacy legislation around the world including the most recent statutory and non-statutory data protection provisions currently in force in Canada. Stemming from this, he summarizes the inconsistencies and inadequacies in the present situation. He is currently undertaking a contract with the CSA to study implementation options for the certification and registration of its model code. He hopes to be able to feed his ideas into the Advisory Council process.

A recent survey "Privacy Revealed" is summarized. It showed that while 52 percent of Canadians are extremely concerned about privacy, 92 percent expressed at least moderate concern. Moreover, 83 percent strongly believe that they should be asked for their permission before an organization can pass on information about them to another organization, and 71 percent totally agree that privacy rules should apply to both government and business. Also, "there is a pervasive sense that personal privacy is under siege from a range of technological, commercial and social threats". Furthermore, greater concern was expressed about business sector organizations than about public sector organizations.

In the review of data protection provisions currently in force in Canada, Quebec is singled out as being the only jurisdiction with general privacy legislation covering the private sector. The provisions of its Act encompass all pieces of personal information collected, held, used or distributed by

another person, confined mainly to enterprises engaged in an "organized economic activity". Its consent provisions cover both the collection and use of personal data, and credit bureaus are singled out as a special type of enterprise. However, it is its provisions re transborder data flow that are seen as having the greatest potential effect outside of Quebec, in that it leaves many unanswered questions in relation to inter-provincial trade, NAFTA, federally regulated private sector enterprises, etc. Consumer credit legislation across Canada is also briefly reviewed. The only other area of the private sector which is seen to have meaningful regulation is telecommunications. In 1992 the then Minister of Communications issued a set of six "Telecommunications Privacy Principles" which were to be implemented by a Telecommunications Privacy Protection Agency made up of representatives of industry and consumer groups. However the Agency never got of the ground for a number of political, economic and practical reasons. This has now been overtaken by the new Telecommunications Act which gives powers to the CRTC to regulate the protection of the privacy of individuals.

Private sector efforts at self-regulation are also reviewed. Codes issued by the Canadian Direct Marketing Association, the Canadian Bankers Association, the Canadian Life and Health Insurance Association, the Insurance Bureau of Canada, and the Cable TV Standards Foundation are described. As well, the efforts being made by the CSA to develop a model privacy code is seen as a most encouraging development.

In reviewing the history of voluntary codes, he concludes that they can help raise employee and consumer awareness of privacy, they are adaptable to different business needs, and can provide some recourse for the average citizen. However they are not binding and most offer no third-party arbitration for complaints. He notes that we have regulated the information practices of almost every public sector institution, and left some of the biggest gatherers and users of personal information virtually unregulated. The rights and interests of individuals can be equally compromised by faulty records in either sector. Therefore, he sees no reason why the same privacy principles should not also be applied to the private sector. He sees three compelling reasons for this: shifting organizational functions in response to new technology practices; strong public privacy concerns (mentioned above); and, the emerging international standards for transborder data flow.

He notes the shifting and imprecise line between the public and private sectors. Where each begins is becoming increasingly difficult to determine. Therefore, he predicts that questions raised about the application of the federal and provincial legislation will have an evolving impact on the practices of the private sector. Increased publicity on privacy issues by both privacy commissioners and the media will also have a spillover effect. Similarly, the privatization of government functions will lead to increased exchanges of data between both sectors, and the matching of data, e.g.,

government data on welfare recipients with bank or financial records to ascertain eligibility, will also narrow the gap. Finally, the pervasiveness and flexibility of the new technologies will make it difficult to determine when data is in the public sector or in the private sector.

Perhaps the most important factor is the new data protection rules emerging from Europe. The proposed EC directives seek to harmonize all European data protection legislation at a high level in order to facilitate trade. Although the previous OECD data protection guidelines had a minimal impact on Canada, the proposed new directives could prove an entirely different prospect for Canadian business. Of particular concern are the restrictions on the transfer of personal data outside the EC. In principle, such transfers are only allowed if the receiving country offers "adequate" levels of protection. The latest draft of the directives represents a weakening from the "equivalent" levels called for in the original draft. Nevertheless, it is probable that only Quebec would meet the new standards, whereas the hodgepodge of voluntary codes and principles in the rest of Canada would not. Such restrictions could lead to high-tech battles over the right to process personal information. Certainly, other countries, including Hong Kong and New Zealand, have taken the situation seriously enough to produce data protection laws based on the European model.

The British Columbia Public Interest Advocacy Centre

The Centre believes that privacy is a right which must be protected and should not be left to be determined by market forces. Therefore, national legislation, inclusion of privacy protection measures in new technologies and consumer education are all options that the government must pursue. Voluntary codes and standards are not strong enough to protect privacy. The Centre hopes that their will be a forum to make more specific recommendations as the government develops options for privacy protection.

The Centre is concerned that it has been suggested that consumers should be able to decide how much privacy they are willing to give up vis-a-vis buying power. This could lead to privacy being treated as an "add-on" to the price and thereby being only of benefit to those who can afford it and to those who are educated enough about privacy issues. Moreover, consumers should not have to make a choice between convenience and privacy. In terms of public concerns, reselling of information should not be permitted without express consent.

Approaches

I. Legislation and regulation is seen as the most important of the possible approaches outlined in the Discussion Paper. Although not

a high government priority, the Charter, when amended, should include privacy as a constitutionally protected right. However, the Charter does not apply to the private sector, therefore other measures are needed. National legislation is needed because provincial or sectoral legislation will lead to differing levels of privacy protection. At the very least, the government should extend the Privacy Act to federally regulated industries. However, federal legislation is needed so that there are no disparities between regulated and non-regulated industries. This could lead to disparities with provincially regulated industries, therefore the provinces and the federal government must work together to ensure that privacy protection applies equally to all Canadians. Moreover, under the Telecommunications Act, the CRTC could mandate that all licensees and applicants have to follow privacy guidelines when offering new services. This would involve bringing all network service providers not currently regulated under the CRTC's jurisdiction.

II. In spite of the efforts made by the Canadian Direct Marketing Association and the CSA to develop voluntary codes, effective enforcement is difficult. The proposed Telecommunications Privacy Protection Agency has not materialized into any kind of effective role. Therefore, voluntary codes and standards are not seen as strong enough to protect privacy.

III. A number of suggestions are made re technological solutions. Hardware and software for the information highway must be designed to provide privacy protection at the outset, it is cheaper at that stage, thus not inhibiting technological innovation. Government could work with the private sector to devise privacy safeguards, legislate privacy standards and, subsidize software in terms of privacy protection. Privacy assessments could be instituted by the government for the introduction of new technologies. There must be opportunities for public participation in the development of privacy threatening technologies.

IV. Canadians must be educated so that they may understand their rights and the consequences of giving out personal information.

Consumers' Association of Canada (CAC)

In summary, CAC favours legislation and sees voluntary codes as only an interim step in the development of such legislation. Also, it believes there is an important role to be played by technological solutions and consumer education. A number of principles related to effective privacy protection also are provided.

Answers to Questions

1. CAC firmly believes that consumers have a fundamental right to information self-determination. The following principles, based on the OECD guidelines, can be applied to the private sector:

   - collect only the minimum information;
   - collect only from the person concerned and specify the purpose;
   - in the absence of consent, use only for the purpose specified;
   - in the absence of authority or consent, do not divulge the information to third parties;
   - ensure that information is as accurate, up-to-date and complete as possible;
   - keep information secure;
   - provide access and correction rights;
   - destroy data when no longer required;
   - make someone responsible for seeing that the rules are respected.

   Other data protection principles, devised by Dr. David Flaherty, also are listed and seen as useful.

2. Stronger privacy protection and security measures are seen to be necessary. This will require a legislative approach involving as little bureaucracy as possible and the most low-cost and efficient operation. Voluntary codes can be used as a foundation on which to build legislation, and both technological solutions and consumer education have a part to play.

3. Federal legislation is seen as essential in order to establish national standards that will decrease consumer confusion and enable all players to compete fairly. In the absence of national standards, CAC doubts that provinces alone will be able to agree. In turn, this might lead to provincial competition for business from companies seeking relaxed privacy protection guidelines.

4. Voluntary privacy guidelines, developed by business, would only be appropriate as an interim step to national privacy legislation.

5. The information highway should be designed to provide high levels of privacy protection. This will not slow the pace of innovation. In fact, it would be more costly to retroactively develop privacy protection systems.

6. Increased involvement of Canadians in the design process is dependent on the effectiveness of consumer consultation. Privacy advocates must be given a seat at the table during the entire design process. In addition, there should be increased consumer representation on the Advisory Council.

7. CAC agrees that Canadians must become better informed on privacy issues. It does not believe that it is the responsibility of business to educate the public. Rather, there should be consumer education courses in schools, colleges and universities. Moreover, information should be available in public and academic libraries.

In closing, CAC quotes from its 1992 background paper "Privacy and Data Protection". The paper lists a number of remedies that require serious consideration if consumers are to feel confident that their personal information is well protected. The remedies include provisions for: consumers to become better informed partners in the use of their personal information and to know who is selling their information, coupled with the right to opt-out; a limitation on the use of credit reports in the employment context; a 30 day reinvestigation of complaints; the licensing of credit reporting agencies by all provinces; the establishment of a privacy protection regulatory agency; and, the establishment of a privately funded, toll-free, national consumer protection "hotline".

The Consumers Council of Canada

The Consumers Council of Canada is an independent non-profit organization. Its mandate is to work in partnership with business, government and special interest groups in order to influence the marketplace. The Council is organized to educate and inform consumers, business and government alike about their rights and obligations.

Overall, the Council is of the view that there must be a legislative framework covering both the private and public sectors which could be coupled with effective voluntary codes, technological solutions and consumer education. The Council looks forward to receiving the analysis of comments received.

The Council lays great stress on consumers rights in relation to privacy on the information highway. Its response is based on the fundamental premise that individuals have sole rights of ownership to their personal information and rights to control its use.

Because consumers are not clearly aware of what information about them is held by various institutions, the uses to which it is put and shared, how long it is held and how secure it is, and because they wish to be able to access this information to ensure its accuracy, there is a high level of concern over privacy issues. The main concern relates to control over personal

information and the uses to which it is put. In this regard, the Council believes that if there was informed explicit consent to its use by any institution, quite apart from any contractual arrangements with the institution, there would be less concern.

Given these concerns, the government should also move to establish order in its own house. Information must not be shared without specific consent. Also, because governments, as well as the private sector, are sellers of information there should be an independent data commissioner. Moreover, model privacy legislation covering the federally regulated private sector should be enacted in 1995.

Approaches

I. There must be a legislative framework to set the standards of privacy for the information highway with an emphasis on prevention of abuses, rigorous standards for protection, a high degree of security and a process for informed consent. The time for action is now. The time for lengthy consultations is long past.

II. Voluntary codes must demonstrate that they can enable individuals to exercise control over their personal information. The ability of industry groups to police their members and influence non-members is questioned. If codes can demonstrate that they can provide consumer protection, they deserve to be given legislative backup.

III. Technology can provide partial safeguards for an individual's information. Such safeguards must be an essential part of the service and not an expensive add-on, thus being universally available. The federal government should encourage new technological developments in this area as this would provide support for home-grown solutions and opportunities for Canadian industry.

IV. There is a large and continuous education/awareness task which both business, government and advocacy groups must tackle. Consumers need to be educated if they are to participate in preventing abuses.

Answers to Questions

1. The following principles should be included:
   - privacy is a fundamental right;
   - the individual is the sole owner of personal information about themselves;
   - only essential information should be collected;

- the individual must give specific consent to the use of their information before it can be used;
- this consent must not be tied to other contractual obligations;
- the information collected must only be used for the purposes for which it was collected;
- individuals have the right to see and to correct personal information;
- privacy protection should be incorporated in new information technologies before they are approved for general use; and,
- there should be no additional cost to consumers to maintain their privacy.

2. Legislation is definitely needed to cover the private sector. Legislation covering the public sector should be strengthened. The government must act now and not wait for federal/provincial agreement (which could take 10 years), or for the completion of " a dialogue to work toward solutions". Legislation could provide backup for effective voluntary codes. If possible, legislation should prevent abuse. If, however, abuse occurs, authorities should act quickly to stop abuse.

3. National minimum standards are essential. Individuals are confused by the current patchwork of regulation and codes. A national standard would enhance the marketplace. However, existing standards should not have to be lowered to meet a national standard.

4. Guidelines are just that, they can probably never be totally appropriate. However, if guidelines are rules and can be shown to work, they may be an acceptable part of the solution. The onus must be on each sector to demonstrate the effectiveness of its guidelines.

5. Levels of privacy protection must be high and fail-safe. High standards do not inhibit innovation, however, even if the pace of innovation is slowed or costs are greater, they are not reasons to deny high levels of privacy protection. Experience with the Swedish product standard is a case in point. Once a standard is set, it will be next to impossible to change.

6. The information highway is not governed by national boundaries. An international forum, in which Canadians must be involved to ensure that our cultural values and concerns are satisfied, will have to deal

with electronic technology and privacy. Technologies and services must satisfy Canadian privacy concerns and designers must know what Canadian concerns are.

7. Consumer education is critical and must be constant. Both government and business have a role to play, particularly in everyday business practices. As well, consumer advocates and the media must strive to raise awareness.

Specific Proposals and Recommendations

Legislation should have provisions to confiscate all profits and return them to victims.

Collecting the opinions and reactions of consumers to privacy matters and solutions to perceived problems must be done. The Council would welcome an opportunity to discuss such a project and could draw on its Canadian Consumer Network to gather opinions.

The potential for electronic spying, fraud and harassment is very real and should not be ignored.

Fédération nationale des associations de consommateurs du Québec (FNACQ)
L'Association coopérative d'économie familiale du centre de Montréal (ACEF-Centre)
(Joint Submission)

Both FNACQ and ACEF-Centre have been active for several years in the area of privacy and personal information. Through their participation in developing the CSA standards and other privacy related projects, they have demonstrated their expertise and willingness to help develop concrete solutions to the questions raised by the issue of privacy on the information highway.

In summary, both respondents are of the view that legislation is essential. Voluntary codes, technological solutions and consumer education can not, by themselves, guarantee an adequate level of privacy protection, however, they all have a part to play.

All studies of the last few years have confirmed that Canadians are very concerned about the protection of privacy and personal information. These concerns are being intensified by the development of the information highway.

Approaches

I. With the official adoption by Canada of the OECD guidelines, they believe a legislative framework is needed to ensure compliance with the guidelines. This will be very complex but by using the example of the Quebec law dealing with the protection of personal information in the private sector, a framework can be put in place that will be applicable across Canada. This framework can be further adapted, by subsequent regulations and codes, to suit the needs of the various industrial sectors. A legislative framework will also create an equal level of obligation on all businesses and will ensure a minimum, universal standard of protection for individuals.

In their view, because the federal government regulates key sectors (banking. communications, and interprovincial and international trade), it must take the lead in establishing a coherent effort across the country to deal with the issues of privacy and personal information. Moreover, the provinces not only have a moral obligation to participate in the process, but, in doing so, will provide economic advantages tied to the protection of personal information both at home and abroad.

II. While voluntary codes can provide some benefits, they are not sufficient to guarantee a satisfactory level of protection. A study by the Centre pour la défense de l'intérêt public, entitled Voluntary Codes: a Viable Alternative to Government Legislation identifies the following deficiencies in voluntary codes: low consumer involvement in development; no consumer participation in administration; lack of administration at the corporate and industry levels; lack of use of publicity as a tool of conformity; lack of universality of application and acceptance within an industry; inadequate monitoring of compliance; weak sanctions; and, lack of effective consumer recourse.

Voluntary codes which are put in place with the involvement of government tend to be more responsive but still have problems, most notably, lack of effective sanctions. Thus, in general, voluntary codes are: not well known, even within the sector which they control; not mandatory within the sector; developed without any consumer involvement; and, lacking in independent organizations to ensure compliance and mediate conflicts. Therefore, voluntary codes will never be enough to satisfy the needs of consumers.

The Québec Consumer Protection Act has a mechanism whereby corporations can submit the equivalent of codes of conduct to the Office of Consumer Protection and, if accepted, the codes must be complied with. The Act also allows the government to extend the

application of a code, modified in detail by members of the industry, to an entire economic sector, the violation of which entails fines and legal sanctions.

III. At least part of the protection must be provided by technology itself. Encryption and coding techniques must be carefully studied and these techniques must allow secure, anonymous access to the resources provided by the information highway.

It is imperative that consumer and civic groups be represented during design, testing and implementation of new products and services. These groups must be financially supported to ensure high quality input with relevant expertise. Social impact assessments of new technologies must be utilized in every sector of the economy and these must be carried out by regulatory bodies before approving new services and products. In this way, costly and time consuming future modifications, as well as confrontations with consumers, can be avoided.

IV. The onus for the education of the users of the information highway must be shared by all parties involved, government, industry and the users themselves. The mandate and resources of the Privacy Commissioner should be expanded to include education. This should include setting up an information centre, periodic public awareness campaigns, and the coordination of the efforts of all the ministries and organizations which regulate industry to ensure compliance to laws and regulations. Information brochures aimed at all levels of education should be produced. Providing these brochures and tools to secondary schools will ensure that future generations will be aware of their rights with respect to privacy and personal information.

Consumer and civil rights groups should be used to distribute information to consumers. Consequently, these groups must be provided with the resources to ensure that they can remain abreast of all the relevant problems and solutions, of technological innovations, and of dispute resolution mechanisms.

Industry must also inform consumers about legal rights and obligations, about practices and guidelines concerning the relevant industrial sector, and about legal remedies available to consumers.

Answers to Questions

1. The principles should be those found within the 1981 OECD guidelines, and those which have evolved through the process of putting these guidelines into practice.

2. The government must enact stronger legislation to counteract the increasing danger of breaches of privacy and to quell the increasing fears of citizens. Outdated practices must be modernized. Only an approach which is carefully thought out and which carries judicial force can resolve the issues and problems.

3. A national level of protection is required to deal with the areas that fall outside of provincial jurisdiction. A global approach is preferred to one which acts on a sectoral basis, because the underlying issues are the same across sectoral boundaries.

4. Voluntary codes can play a role providing that they conform to legislative standards.

5. The information highway should be designed with a high level of privacy protection. Experience has shown that it is very costly to try and modify an existing system. The methods and techniques used to ensure high levels of protection will not have a significantly negative impact on the pace or cost of innovation.

6. Participation by Canadians is essential in the implementation of systems which will have an impact on their fundamental rights. This can be accomplished in several ways: participation in the legislative process; appearances before administrative bodies such as the CRTC; and, participation in forums and discussions held by government and industry. Because participants must be properly prepared in order to make a useful contribution, they must be provided with adequate resources.

7. Consumer groups can play an important role in the process of informing Canadians about their rights and obligations with regard to privacy and personal information.

Specific Proposals and Recommendations

The mandate and resources of the Privacy Commissioner should be expanded to include education together with the coordination of government institutions which regulate industry in order to ensure compliance with privacy laws and regulations.

Funding should be provided to permit the involvement of consumer and civil rights groups in education initiatives and public hearings.

La ligue des droits et libertés

The submission of La Ligue covers two main issues. Its general interests, and answers to a variety of questions posed in the Introduction of the Discussion Paper and in Part 2, "Privacy Issues for the Information Highway". In summary, it believes that legislation must be enacted that will ensure a minimum level of privacy. Voluntary codes are seen as being unable to address the needs of all parties, and favoured technologies should be the ones that collect the least amount of information for the particular task. La Ligue looks forward to receiving the analysis of comments received. Also, it expresses an objection to the relatively low weight given by the Advisory Council to individuals and consumer protection groups, as compared to that given industry.

In regard to the general interests of La Ligue, the main issue relates to its belief that the definition of privacy given in the Discussion Paper is too limited because the issues raised by the introduction of the information highway involve much broader concepts. It believes that the definition must be expanded to include concepts of:

- privacy, as it deals with of the right to live in peace without interruption or intrusion ;
- reputation, a right guaranteed by the Quebec Charter;
- dignity, also guaranteed by the Quebec Charter;
- democracy, as it applies to the sharing of power and control over one's information, involving informed consent to collection, use and disposal.

Equally, an end must brought to the concepts of the State as the sole and primary protector and of industry enjoying hegemonic control over personal information, a resource which does not belong to it.

In the opinion of La Ligue, individuals must have a greater role in protecting their information and in dealing with problems which might arise from its dissemination. This involves such areas as consent for medical procedures, and consent to allow the use of personal information to further the public good, i.e. medical research. In addition, a system, where the most glib, or the best informed, can prevail simply by convincing one person, must be opposed. In order to bring these changes about, it is not imperative (nor is it possible) that each individual have access to all relevant information. What is important is that the infrastructure, services, and conditions do not favour monopolies or oligarchies but are completely democratic in nature. The challenge is the social integration of everyone in a complex society.

La Ligue also proposes that, in order to ensure that the knowledge gained by science and technology does not lead to the social exclusion of any

individual or group, we must question the rationale that underlies the exclusion, the level of trust in the information that leads to the exclusion, and methods employed to use the information. In relation to information about an individual, we must be able to differentiate between facts which are known to be true, as opposed to those which are only possibly true. Therefore, we must guard against legislation which may entrench inequalities, or perceptions of power, between industry and consumers. In overall terms, protection of personal information is placed mid way between privacy, reputation and dignity.

In regard to the second main issue, answers to the variety of questions posed in the Discussion Paper, La Ligue makes the following points.

On the question of the respective roles of government, business and individuals, it believes that there must be optimal control of their information by individuals. Laws that set out the general principles of the standards of information management are too general in nature. The government ought to assume its responsibilities and adopt sectoral regulations which stem from negotiation between industry, government and individuals.

On questions relating to transactional data and personal profiling, it believes that, because of the differences in power of the players, equilibrium between the advantages and dangers will not come about on its own. Legislation must be enacted which will ensure a minimum level of privacy. It is the balance of power between the players that is the issue. Moreover, all individuals must be guaranteed total access to any personal information which relates to them because it is, in effect, part of them.

Relating to identity cards and unique identification numbers, La Ligue believes that the erosion of liberties does not come about because an individual must divulge relevant information to complete a financial transaction, nor from the assigning of a unique identifier to an individual. The erosion occurs when the individual loses control over information once it is transferred to an institution.

On monitoring and surveillance, La Ligue has firm views. The key issue is to define the extent of a personal "protected information space". Different types of information require different security requirements. The information highway must be able to accommodate all types of information and the resulting security needs, from non-security bulletin boards to financial transactions. However, even in the areas with the least security, steps should be taken to ensure that personal information profiles can not be compiled without the individual's consent. In addition, all forms of surveillance used to measure the productivity of workers should be banned because they contribute to the disempowerment of the individual and the dehumanization of the work place. These methods are also counter-productive. The best measure of productivity is the amount of work done.

Also, strict regulations must be in place to ensure that information gathered in the process of providing protection for a household is not transferred to a third party and that only pertinent information is gathered.

In regard to intrusion, it is the opinion of La Ligue that the forms of intrusion referred to in the Discussion Paper, such as telemarketing and targeted advertising mail, are fairly inoffensive, as long as the intrusion is as a direct result of an action that the individual has taken. This issue is dealt with adequately by the Quebec law on the protection of personal information in the private sector.

Approaches

II. It is believed to be essential that any codes and standards apply universally and that there be no provision for the transfer of information for profit, much as it is currently illegal to sell human organs, even with the individual's consent. Voluntary codes of conduct can not properly address the needs of all parties because of the conflicting interests of individuals and corporations.

III. La Ligue strongly believes that technologies must be developed to ensure that the individual is in full control of information, choices and consent processes. These technologies must be flexible enough to ensure full freedom of choice for the individual and be reliable when dealing with social standards. Favoured technologies should be the ones that collect the least amount of information possible for the particular task. Monitoring mechanisms should exist to ensure that all information management procedures meet the required public levels. As well, the public hearings approach is slow and costly, yet provides some benefits which cannot be derived through telephone surveys, etc. The responsibility for protection of privacy and personal information must be spread among all the players to ensure the resulting technologies do not infringe on civil liberties. In the light of experience, certain aspects of privacy protection will require legislation, whereas others can be on a user-pay basis.

Public Interest Advocacy Centre (PIAC)

In summary PIAC contends that legislation/regulation is required, complemented by voluntary codes, technological solutions and consumer education.

Concern is expressed that the privacy concerns of lower income Canadians, e.g., having to pay for access to their personal information, and for maintenance of existing levels of privacy, may not be given adequate attention. It also is noted that the increasing public concern about privacy, as reflected in recent surveys, is justified.

Answers to Questions

1. The following is a list of privacy principles:

   - a definition of "personal information" which includes all information about an individual;
   - personal information, like private property, belongs to the individual;
   - individuals have a right to know whenever their personal information is collected, used, shared, traded, or disseminated in any way;
   - individuals have a right of access to their personal information and to have any erroneous information corrected;
   - individuals have a right of control over the collection, use and distribution of their personal information;
   - citizens should not have to pay to maintain a pre-existing level of privacy;
   - low income Canadians are especially vulnerable to privacy invasions and their special needs must be recognized.

   The principles in the CSA model privacy code also provide a good basis for a set of guiding principles.

2. The federal and provincial governments need to introduce privacy legislation covering both the public and private sectors. Legislation/regulation is required, regardless of how well industry self-regulation appears to be working. The federal government should begin by drafting national or sectoral legislation for areas under its jurisdiction. This exercise should be done in concert with provincial counterparts, including all privacy commissioners, to create a common set of rules for all sectors. The recent Quebec law would provide a useful model.

   In addition, the federal Privacy Act should be amended so as to require "privacy impact assessments" on all new government initiatives, in a non-cumbersome manner. Such up front assessments should be cost-effective in avoiding expensive corrections at a later date. Consideration also should be given to legislation which would make such assessments mandatory for the private sector.

   Legislation should be guided and complemented by voluntary codes, but such codes cannot, and do not, substitute for government regulation. PIAC has published a study on the effectiveness of voluntary industry codes and found them to be lacking in consumer

awareness, adequate coverage, adequate sanctions, and systematic procedures to measure and monitor compliance.

New cryptology techniques such as "public key" encryption should be aggressively promoted by the government.

Government has a role to play in raising the level of awareness both of existing laws and existing risks involving privacy.

3. National and provincial legislation, preferably harmonized, is necessary. However, differing levels of privacy protection is better than none at all. Equally, omnibus legislation is preferable to sectoral legislation. Nonetheless, the latter is better than none at all.

4. Voluntary codes are worthwhile in that they: raise industry awareness; have the potential to raise public awareness; help industry to "get up speed" before legislation comes into effect; and, can aid drafters of legislation with ideas and guidance on appropriate principles, sector-specific privacy issues and possible means of implementation. There actual effectiveness is less clear, nevertheless they should be encouraged.

5. The information highway should be designed to provide high levels of privacy protection even if it costs more and slows down development. However, additional costs are not anticipated because early built-in privacy protection should be less costly in the long run.

Charles D. Raab

Charles Raab is a Senior Lecturer in the Department of politics at the University of Edinburgh in Scotland. He is an academic researcher into issues of privacy and data protection.

Although acknowledging the constitutional and legal obligation to be overcome, he believes that it is essential to provide a more comprehensive and systematic framework of regulation to cover the private sector. Although the voluntary code approach has much to commend it, it cannot be the whole answer. Also, he sees technological solutions and public education as having partial but important roles. In summary, he sees the various approaches in the Discussion Paper as being complementary and intertwined.

Approaches

I. Legislation is an important way of strengthening individual rights and organizational responsibilities. Moreover, vigorous regulatory agencies are required if the law is to be enforced. It is instructive to note that the latest draft of the European Union directive abandons

the ill-conceived public/private distinction because personal data flows between those sectors in a way that renders the distinction increasingly irrelevant in practice. In this regard, Quebec's coverage of the private sector strikes a positive note.

II. The voluntary code approach has much to commend it, e.g. the UK and Netherlands experiences. One problem may be the identification of relevant industries and sectors. The new multimedia opportunities on the information highway may blur the line between industries and sectors, bringing the applicability of sectoral codes into question. However, the CSA approach may be seen as a breakthrough, particularly in regard to serving as a measure against which compliance could be assessed by the EC.

III. Technological solutions also are attractive. However they are only a partial answer because privacy requirements go far beyond technological solutions. In addition, it is important that technological safeguards be built in rather than bolted on. Moreover, privacy impact assessments and their consideration in a public fora would be valuable.

IV. Education involves the realization that privacy protection may ideally be the result of collaboration among differently placed participants with different interests. Thus, education can result in a synergy of seemingly competing interests.

Riley Information Services Inc.

Riley Information Services are international specialists in the creation of public policy on information issues. Thomas B. Riley, its president, also is well known for his writings and the organization of conferences on matters relating to privacy and access to information.

In responding to the Discussion Paper, Riley Information Services has submitted a copy of its paper "Information Technology and Privacy Protection: Practical Suggestions for the Information Age" which was presented to the Electronic Democracy Conference in November, 1994.

The paper reviews the types of privacy protection challenges posed by information technology and traces in detail the development of privacy principles, regulation and legislation both in Canada and abroad. It also highlights the manner in which developments in Canada are lacking in terms of meeting the demands of the "Information Age". An attempt is made to raise some substantive questions about the nature of privacy protection principles, appropriate forms for such protection in the private sector, and ways to improve current measures in the public sector. In doing so, it sees the Privacy Act as the pre-eminent national authority for privacy

protection and suggests for consideration a number of amendments to the Act. At the federal level, it reviews how the federally-regulated private sector may be brought into the equation, and in the public sector, how privacy and security concerns may be built into the information systems development process. Finally it deals with issues related to the use of the SIN, data matching, federal/provincial exchanges of personal information and commercialization of public sector personal information.

The definition of privacy is traced from the American jurists Samuel Warren and Louis Brandeis, through Alan Westin, thence to David Flaherty. Westin's approach is seen as being the basis of current federal and provincial privacy legislation.

The fact that there are real privacy concerns and that threats to privacy are growing is well documented. Technology now has the ability to manipulate data in ever more sophisticated ways, from the creation of "data shadows" to new forms of electronic surveillance of employees. Personal information is now commercialized for many purposes, including market development. Governments are more and more sharing personal information, all in the name of efficiency and effectiveness. All of which stimulate increasing privacy concerns in the general public. The recent controversies over such events as the Lotus CD-ROM project in the USA, the Law Enforcement Access Network in Australia, the health care identification proposals in Ontario, and the PharmaNet proposals in British Columbia, all indicate that the perceived threat is increasing. Nevertheless, it is recognized that customers do want new and innovative services and are supportive of the use of technology to combat crime and fraud. This leads to a strange ambivalence in that Canadians are more solicitous of ensuring their own privacy protection than that of their fellow citizens. Moreover the information highway will bring incredible benefits to all parts of the country, particularly in the realms of access to information databases, education and medicine.

In relation to these privacy concerns, a number of specific privacy issues are dealt with. The widespread use of the SIN is seen as a continuing problem, in that it symbolizes the possibility of "big brother". surveillance. Data matching, in terms of its ability to reduce fraud and aid in crime detection, as opposed to its privacy invasion capabilities, is an unresolved dichotomy both in Canada and abroad. The federal-provincial exchange of personal information to eliminate overlap and duplication of programs and services continues to cause concerns, in spite of the potential benefits. Commercialization of personal information, particularly by the government in an attempt to reap additional revenues, still remains an issue. Suggestions are made that all of these issues could be dealt with, first by amendments to the Privacy Act, and possibly by other legislation in consultation with the provinces.

Canadian and international experiences in the development of privacy protection measures also are reviewed in detail. These range over a wide spectrum. In Canada, they include: the evolution of the Privacy Act and its evolving problems; the promulgation of the Telecommunications Privacy Principles and subsequent amendments to the Telecommunications Act, coupled with resultant privacy protection decisions of the CRTC; the abortive attempt to bring the administrative arms of the Senate, House of Commons and the Courts and all federal crown corporations under the Privacy Act; and, various provincial initiatives, particularly the recent Quebec legislation which regulates privacy protection in the private sector. International experiences are traced from the OECD guidelines in the early 1980s to the proposed EC privacy directives. Current initiatives in the USA, such as the attempt by the NII Task Force to develop general privacy principles for use on a national computer network, also are discussed.

The privacy principles of the OECD Guidelines are seen as the most important influence on the development of Canadian privacy initiatives. However, in the light of developments in technology and the more sophisticated uses of personal information, they need to be updated. The NII proposed principles, in the USA, are not seen to be strong enough. The general criteria of the federal Privacy Commissioner for the development of government personal information systems, which involve the concepts of openness, informed consent and security, are seen to have considerable merit. Equally, the proposed CSA Model Code for the Protection of Personal Information in the private sector is seen to be important. However, it is contended that one more principle can be added. This involves pushing public input back to the planning or initiation stage of personal information systems.

The need for additional legislation and regulation concentrates on proposed amendments to the federal Privacy Act which is viewed as the pre-eminent authority for privacy at the national level in Canada. These potential amendments include: incorporation of a basic set of privacy principles; the inclusion of crown corporations and the federally regulated private sector, with review, approval and complaint mechanisms attached to the office of the privacy Commissioner; a new definition of personal information to include electronic and other surveillance, as well as genetic information; provisions for the annual review of the Privacy Commissioner's Report by a parliamentary committee, similar to the review of the Auditor General's report by the Public Accounts Committee; a general clause on protective measures and a more specific requirement for security and privacy impact assessments, etc. Three options are reviewed for the control of privacy protection in the private sector: legislation similar to the Quebec legislation, seen as too much of a blunt instrument; continuation of voluntary codes, complemented by the CSA model code; allowing sectoral issues to drive

privacy protection on a case by case basis. However, a compromise option is suggested. The Privacy Act would require private sector companies to develop privacy codes, based on the CSA proposed standards.

Voluntary codes, with the possible exception of the banking, direct marketing and cable industries, are not seen as a success to date. However, they have the advantage of flexibility to meet changing needs and sectoral differences. Moreover, Industry Canada activities appear to herald a sectoral approach, as do the Senate hearings on the Bank Act. Equally, consumer pressures and CRTC privacy decisions could all lead to their greater adoption and effectiveness. Unfortunately, they could lead to "balkanization" and leave major gaps in privacy protection. Nevertheless, the adoption of the proposed CSA model privacy code as a national standard is seen to have considerable merit.

Technology is seen as basically neutral. Nevertheless, both in terms of initiatives to re-invent government and in the general private sector, potential threats to privacy are evident. However, they are coupled with many technological solutions that aid privacy protection, such as smart cards and encryption. Nonetheless, the key is seen as providing for privacy concerns and building in protection measures at the development stages of information systems. Considerable detail is provided as to just how this could be accomplished, including a step by step process, involvement of the Privacy Commissioner's office, and the adoption of security and privacy impact assessments.

Leslie Regan Shade

Leslie Regan Shade is a member of the Graduate Program in Communications at McGill University.

The submission consists of part of the recent article on Computing Networking in Canada in the Winter, 1994 issue of the Canadian Journal of Communications. The article discusses legal issues in networking, privacy platforms for networking in the USA, and provides some suggestions for Canadian privacy legislation for networking. In regard to the latter, it suggests that Canada might look to the US Electronic Communications Privacy Act (ECPA) of 1986 and the European Community's draft Telecom Directive when regulatory agencies plan their equivalent. Also, in the light of proposed CANARIE initiatives, it would seem advantageous to extend the 1992 Telecommunications Privacy Principles to networked communications by adapting aspects of the ECPA, the EC Telecom Directive or the privacy principles of the Computer Professionals for Social Responsibility.

Canada Trust

Canada Trust is the commonly used name for the Canadian operations of CT Financial, Canada Trustco Mortgage Company and its subsidiary The Canada Trust Company. It offers services in all ten provinces in the areas of savings and loans, personal and pension trusts, residential real estate brokerage and retail financial services.

Canada Trust has always given the highest priority to the protection and confidentiality of personal information concerning its clients. It favours self-regulation and voluntary privacy codes over legislative solutions. More specific comments related to the financial services industry can be provided in the future if required.

Legislation is not favoured. However, if legislation is considered necessary, it is important that it strike a balance between the protection of privacy and the free circulation of information which is so necessary in a market economy. Legislation such as the Quebec act does not strike this balance and is not recommended. The new Bank, Insurance Companies and Trust and Loan Companies Acts authorize the government to make regulations on the use of customer information. Consumers of financial products have not besieged the government with complaints of abuse of confidential information. Therefore, there has not been a need for regulation.

The trend in Europe and federally in Canada is seen as being toward self-regulation and monitoring of industry by having various sectors implement voluntary privacy codes. The banks have developed privacy standards and Canada Trust is in the process of doing so. Moreover, an industry-specific approach would balance the different information and operating requirements of various businesses and the effectiveness of consumer protection.

Canadian Bankers Association (CBA)

The Canadian Bankers Association represents Canada's 62 chartered banks.

In general, CBA does not favour legislation. It believes that self-regulation and voluntary privacy codes are a recognized and well-suited structure to protect privacy, particularly in the ever-changing electronic banking environment. Consumer education and technological solutions are also seen as an important part of the privacy equation. The submission also briefly reviews the various banking applications currently in use on the

information highway and expands on them in the accompanying document "Canadian Banks and the Information Highway" which was submitted to Industry Canada in 1994.

Protecting customer privacy, confidentiality and security is fundamental to a banks business. In this regard, banks and their customers recognize that the delivery of products and services involves the use of customer information. Developments in banking are customer driven. Thus, the success of the information highway will depend on satisfying various consumer needs and service expectations and in addressing customer privacy considerations. Therefore, it is suggested that further and careful assessment of the issues is required before acting on privacy considerations that could have repercussions for the development of the highway.

CBA believes that legislating privacy could inhibit innovation in the marketplace which is the driving force behind the highway's development. Moreover, Government regulation of privacy and information use could hinder the adoption and promotion of self-regulatory codes. Furthermore, legislation is substantially less adaptive than self-regulation and should not be designed to achieve "micro-management" of business standards.

Organizations must take a leading role in self-regulating and addressing privacy and security. In turn, Government must facilitate and encourage self-regulation and promote responsible decision-making by consumers. Banks are leaders in self-regulation in that the CBA,s "Model Privacy Code for Individual Customers" has been adopted by banks. Also, many banks subscribe to the Canadian Direct Marketing Association's privacy code, and the Canadian Debit Card Code of Practice. As well, banks provide toll-free 1-800 numbers for customers to voice their complaints and concerns. Moreover, self regulation can overcome jurisdictional hurdles where federal and provincial interests may hinder the adoption of one set of agreed-upon rules, and voluntary codes can help businesses deliver minimum service standards. Furthermore, self-regulation offers the greatest flexibility to adjust practices to changing client needs and expectations and it makes sense to encourage it at a time when the federal government is streamlining the regulatory process. Essentially, individual bank codes are "live" documents subject to routine review and amendment to reflect changes in the marketplace and in customer's attitudes on privacy in banking, e.g. new "opt-out" provisions. CBA also has participated in the development of the CSA model privacy code, however, it is suggests that questions relating to CSA's certification role should be best considered by the CSA committee process.

Many examples are provided on how CBA and the banking industry are participating in the development of new and innovative technologies. All new banking products and services are developed with privacy, confidentiality and security firmly in mind. Not only is technology being

used to protect information and secure systems, but it is being used increasingly to allow customers to exercise their right to further protect privacy. CBA questions the need for regulators to engage public hearings when new technology is brought to market. Also, it is concerned that market innovation would require government sanctioning.

In a self-regulatory environment, organizations have a responsibility to deliver sufficient information to help customers understand products and services in general and to allow them to make an informed choice, at the decision point, about electing to use a particular service. In this regard, the banking industry also is extending its traditional paper-based consumer education initiatives into technology based systems. Customers also have the responsibility to shop around, understand their obligations and take reasonable precautions to protect their own privacy. Government also has a role in supporting consumer education.

Canadian Direct Marketing Association (CDMA)

CDMA represents 575 companies across several industries involved in the direct marketing of products and services across Canada. Founded in 1967, its members include major financial institutions, publishers, cataloguers, charities, televised home shopping services, advertising agencies, direct response agencies, computer and data-management and telecommunications companies, service bureaus, printers, and letter and package delivery services.

CDMA concentrates its submission on the developing role of direct marketing on the information highway. In doing so, it strongly supports industry self-regulation and voluntary privacy codes supported by technological solutions.

A number of points are made in relation to general factors that CDMA sees as being of importance in the development of the information highway. Also, a great deal of detail is provided on such topics as: factors influencing the growth of direct response marketing; the information highway's impact on direct response marketing; consumers and technology; direct marketers and the information highway; do Canadians want to shop from home on the information highway; making informed consumer choices; and, customization.

In summary, the details provided indicate that the direct marketing industry is very large (200,000 employees and $9 billion in sales in 1993) and growing rapidly. As the information highway evolves, many new services will be offered and new markets will open up. Of these, potentially the most important will be home shopping, coupled with interactive technology. In a recent US survey, 89 percent of respondents showed strong support for home shopping. Moreover, as the technology falls into place, direct

marketing will become less intrusive, more informative and will provide greater privacy protection. In the final analysis, the future of the industry depends on building and maintaining consumer confidence in the security of transactional data.

The information that the direct marketing industry uses, mainly purchase records, is not considered at the heart of the privacy issue. The privacy debate has usually focused on the collection and use of personal information such as health and financial records upon which major public and private sector organizations base decisions that affect individual's lives.

In regard to privacy protection measures, CDMA strongly supports voluntary privacy codes and points to its own code as an example. The mandatory 1992 Privacy Code of the CDMA, whose members account for approximately 80 percent of the direct marketing activity in Canada, has helped assure consumers of their right to control the use and transfer of information such as purchase records. It includes provisions whereby consumers can limit access to marketing information to marketers of their choice or deny access entirely, provides the right to know what information the marketer holds , where it came from and the right of correction. It is believed that, given the choice, privacy conscious consumers will opt to deal with organizations that respect their rights to limit uses of personal information. In the final analysis, the most useful information is information that is provided voluntarily because it is more accurate and provides more detail for selective marketing. Also, CDMA has participated in the development of the CSA draft model privacy code and believes that any responsible direct marketing campaign can meet the tests set out in the draft code.

CDMA believes that encryption system will be used to protect data from hackers and to safeguard financial transactions and various forms of paperless payment. As well, security of transactional data is not only in the consumer's interest but is also in the interest of the industry as a whole.

Interac Association

Interac Association was formed to facilitate the exchange of electronic transactions among Canadian deposit-taking institutions. It operates the Shared Cash Dispensing service through banking machines from coast to coast as well as the Interac Direct Payment service.

Consumer polling indicates that privacy protection and security are very important to consumers and therefore critical to the success of any electronic network. In this regard, the two services provided by INTERAC can be used without jeopardizing privacy, specifically by the use of a personal identification number (PIN). The services running through the INTERAC switch provide end-to-end protection for the customers

transaction. Thus, the clear message is that there are very effective systems solutions available which can and should be embedded at the technology development stage. Interac also supports the CSA approach because the proposed model privacy code will enable different sectors to tailor specific codes to suit peculiar circumstances.

Equifax Canada Inc.

Equifax Canada is an information services company which collects, holds, consolidates and communicates information to its customers on individuals and companies to facilitate financial transactions. It operates a computerized network of credit information and a debt recovery services across Canada. Also, it manages separate databases on automobile claims, dwelling insurance claims and loss insurance claims. All activities are independent of each other and the information is kept in separate databases.

Equifax is of the opinion that voluntary codes of conduct will probably settle most of the problems of the protection of personal information on the information highway. If, however, legislative or regulatory solutions were to be adopted, it is essential that they be clear and homogeneous to allow industries to operate across Canada and that they be balanced enough to allow for the evolving nature of the information highway and avoid implementation problems for any new service or technological advance. It is also convinced that technology can offer solutions to some problems, particularly involving security and controlled access. Moreover, it is up to the promoters of the highway to inform the Canadian public of its benefits in a positive light in terms of democratic control, access to information, equal treatment and security of data.

Studies conducted for Equifax and released in 1993 show that Canadians have real concerns about their privacy. They showed that strong majorities: favour the addition of a provision to the Charter of Rights to protect privacy; perceive privacy as a fundamental right; and, are worried about their privacy. Their major concern lies in the way that companies and government agencies can use computer technology to collect, compile, and exchange personal information about an individual. Specific concerns relate to security measures, incompatible uses, customer profiles, cross-border transfers, and inaccurate information. However, an equally strong majority agree that computers give people more convenient access to useful information and services and have improved the quality of life. Moreover, the same majorities responded positively to the use of personal information in setting automobile rates, in approving loans, and in issuing a credit card or establishing credit limits. Furthermore, although Canadians view privacy as a fundamental right, they agree that it must be modulated in the public interest re prevention of fraud and crime, and reduction of debt and bankruptcies, etc. The report concluded that 62 percent of "Canadians take

a pragmatic approach to balancing privacy interests and access to valued consumer benefits. Moreover, recognition of the right of access to their files and the possibility of rectifying errors or adding comments, considerably reduces the public's concerns. Equifax believes that the end result should be a balance of required controls while allowing for the speed of execution and principle of interconnection which are the essence of the information highway.

Equifax believes that certain principles should be followed in attempting to protect personal information on the highway. A framework of standards or rules should be adopted that would cover the collection, holding, use and communication of personal information, and that would provide rights of access and rectification. However, it is essential that these rules be balanced to allow for the evolving nature of the highway. Moreover, they should consider differences in the sensitivity of information, e.g., financial information is of higher sensitivity than customer profiles. Nevertheless, in regard to the latter, consumers should have the right to know their customer profiles and add comments thereto. Finally, data coupling should not be absolutely prohibited but individuals should have the right to opt-out from inclusion in mailing lists.

If legislation is decided upon for the private sector it should establish rules that are clear and homogeneous to allow industries to carry out their activities across Canada, without being caught in the constitutional vice. The federal government might look to the European model by adopting a general framework to which the provinces would be called upon to subscribe. The data banks of both government agencies and private companies should then be subject to the same rules because they will be connected to the same network.

Equifax does not favour additional legislation because for over thirty years it has provided consumers with rights to access their files, to make corrections for inaccuracies and it provides notification to businesses of corrections made. Accordingly, it has had little trouble in meeting the requirements of the Quebec law on the protection of personal information in the private sector. Moreover, it will be essential to adapt applicable laws and regulations to the new reality of the instantaneous nature of transactions on the information highway.

Given its thirty years of experience in privacy protection measures, Equifax considers that it effectively operates a system of self-regulation, subject to the framework of standards and rules set out above. Voluntary codes would take into account the particular circumstances of the various users and would be developed after consultations with consumers. Also, they should be flexible enough to take into account the evolving nature of the information highway and not impose useless legal barriers.

Although there is consumer concern about technology, Equifax is convinced that the new technologies can offer answers to the public's concerns. Computerized databases are more secure than paper files because all usage and unauthorized access can be controlled electronically through such measures as access codes and smart cards. Equifax, itself has strict security procedures in place both for operating and for client access to its system, has an internal code of conduct for its employees, and provides them with extensive training courses. In the development of new technologies, advance consultations with consumer groups could forestall blockage of new projects and the proliferation of lawsuits. Consultation could be through an ombudsman or other comparable agency. An example is given in relation to the current debate on whether fibre optic services should go right into the home or whether they should terminate 100 metres away and then be transmitted by wireless communication. The latter option is less costly but is fraught with privacy protection implications.

Commission d'accès à l'information du Québec

The Commission reviews the effects of the information highway. It strongly supports the role of legislation. As for voluntary codes and technology, they will only be effective if governed by such legislation. In this regard, it attaches a copy of its submission to the study being undertaken by the UBI Consortium.

It believes that the information highway will appreciably change the way of life of Canadians. Many agree that it poses a menace to their privacy, particularly to their personal information which circulates on it. The newly formed consortia, primarily made up of private companies whose goal is to provide information systems, will hold all manner of personal information about individuals, particularly on their habits and lifestyle, which will be of value to business. Individuals will find it difficult to protect such information because of the manner in which it will be circulated and distributed.

In its submission to the UBI Consortium, it discusses the benefits of the information highway, such as: an aid to economic development; an unprecedented means for the government to communicate with its citizens and for them to access government information; telemarketing and tele-education; carrying out financial transactions; etc. However, it cautions that these benefits must be balanced by measures which will protect individuals from undue intrusions into their personal lives (creation of personal profiles) and their homes (surveillance), as well as measures that will allow them to control the collection and use of their personal information (informed consent). In so far as Quebec is concerned, it sets out in detail the provisions of the Quebec laws that protect personal information in both the public and private sectors and to which both sectors must conform.

Approaches

I. The Commission notes that few provinces exercise jurisdiction over the private sector with regard to privacy and personal information. However, in spite of the jurisdictional problems which this involves, it considers that for the information highway, as for any other sector, only a legislative approach, backed by effective sanctions will ensure that the rights of individuals with respect to privacy and personal information are respected. A legislative framework will also contribute to consumer education by identifying the rights and obligations of all parties. The measures enshrined in Quebec law show that it is possible to protect the privacy and personal information of citizens without harming the competitiveness of business or creating obligations which can hinder its operations.

II. It is often stated that voluntary codes are less constraining for business than a regulatory framework. However, the Commission believes that voluntary codes are lacking in several key areas. They are voluntary and some businesses do not adhere to them; no independent and impartial authority assures compliance; and, individuals have no recourse, other than those stipulated in the code.

III. In the view of the Commission, technological solutions can only work where the principle of confidentiality has been enshrined in a legal sense. The highway must be provided with all the technical means required to ensure the protection of personal information. In this regard, security is an important aspect, including cryptography for sensitive information such as medical information. Employees of the system must be made aware of their obligations to protect personal information, including the signing of confidentiality agreements. The security systems, themselves, should include such measures as access codes and passwords, limited access and daily logs, for employees; and, access cards and PINs with automatic rejection for invalid entry, access code modification only at the point of service; and, proper identification when issuing a new or replacement card, for users. Moreover, access by all individuals, regardless of whether they lack technological expertise or are handicapped, should be available in order to ensure that two classes of citizens are not created. Furthermore, impact assessments ought to be carried before any information from the public and private sectors is introduced on the system.

Information and Privacy Commissioner of British Columbia

A combination of both federal and provincial regulatory initiatives coupled with private sector codes, which should ultimately have the force of law and be subject to independent monitoring, are seen as the most likely solution to the question of privacy on the information highway. In addition, the use of technological solutions to safeguard data, along with consumer education also are seen as essential ingredients.

Profiling, linking and matching are critical concerns, given the significant value which is attached to personal data by commercial interests. A more specific concern relates to the ability of individuals to only enter into transactions on the basis of informed consent. Lack of governmental and corporate sensitivity to the preservation of the right of privacy could lead to a significant risk of hostile consumer response to technology developments. In this regard, some privacy advocates believe that the continued automation of traditional public records, such as vehicle registration and driving licence data with their multiple uses and linkages, pose significant threats to the privacy interests of individuals. The potential of new

technologies to allow physical surveillance of individuals also is a concern. The application of fair information practices can take care of most of these concerns.

Although British Columbia, Alberta, Ontario and Quebec are covered by privacy legislation, with some other provinces having less comprehensive legislation, only Quebec has privacy legislation covering the private sector. This compares with the experience in Europe where the EC privacy directive is in the final draft stage. Under the EC directive, protection of personal privacy is established as a basic human right. It covers manual and automated records in both the public and private sectors. Basic principles of fair information practices are established, along with independent review of compliance and legal recourse. Moreover, its data protection provisions could have a negative impact on the EC's trading partners which do not have reciprocal protection measures in place.

The following 12 primary data protection principles and practices for the treatment of personal information are provided

- Openness concerning government personal information systems, i.e., no secret data banks.
- Necessity and relevance governing collection and storage of personal information.
- Reducing the collection, use and storage of personal information to the maximum extent possible.
- Establishment, in advance, of the purpose and ultimate administrative use of personal information.
- Establishing and requiring responsible keepers for personal information systems.
- Control of linkages, transfers, and interconnections concerning personal information.
- Requiring informed consent for the collection of personal information.
- Requiring accuracy and completeness in personal information systems.
- Provisions re data trespass, including civil and criminal penalties for unlawful abuses.
- Requiring special rules for protecting sensitive personal information.
- Right of access to, and correction of, personal information.
- Right to be forgotten, including ultimate anonymization or destruction of almost all personal information.

In more specific terms, transfer of data to third parties should only occur on the basis of a choice to "opt-in" rather than to "opt-out", as is favoured by the private sector. Moreover, informed consent should be as "informed " as possible, and opportunities to allow free choice should be maximized.

There is agreement that "data havens" and interprovincial trade barriers, caused by differing privacy protection requirements, need to be avoided.

It is seen as unnecessary to implement a **uniform federal statutory response** to all of the privacy problems posed by the information highway. A typical Canadian solution will likely involve both federal and provincial regulatory initiatives. A starting point could be the extension of the federal Privacy Act to all federally regulated private sector institutions. Moreover, progressive legislation and regulations should be enacted to cover the enormous information holdings at all levels of government. However, all efforts at regulation should be prefaced by ongoing efforts to understand proposed uses of technology and how they will actually operate.

Every agency and organization holding personal information should engage in as much voluntary self-regulation as possible by means of privacy codes that incorporate fair information practices . However, none have the force of law or are fully responsive to the privacy concerns of individuals. In this regard, attention is recommended to the findings of the current research by Professor Colin Bennett (for the CSA) on the implementation of voluntary codes in advanced industrial societies. In the final analysis, such voluntary codes should ultimately have the force of law with an outside body responsible for monitoring compliance.

It is essential to identify the extent to which any new technology presents an information privacy issue. The preparation of privacy impact statements should be an essential prerequisite to the promotion and application of new technology, products and services by both the public and private sectors. At the very least, they should identify competing interests to the fullest extent possible and suggest how, if at all, a balance may be achieved. While most new technologies present a challenge to personal privacy, they can also provide safeguards to personal data, such as reliance on encryption and smart cards.

Information and Privacy Commissioner / Ontario

The enactment of federal legislation for the private sector is supported as being necessary, along with equivalent provincial data protection measures. Voluntary privacy codes for the private sector are seen as only a first step. Technological solutions can be a part of the solution. Also, public education is deemed to be a fundamental need.

The 1994 Gallup Canada poll done for Andersen Consulting Canada noted that while the majority of respondents (67.7 percent) thought the information highway was a "good idea", an even greater majority (83.7 percent) described themselves as very or somewhat concerned about how the information highway may affect their personal privacy. Therefore, it is necessary to ensure that, along with the benefits, the development of the highway does not quickly and quietly erode the privacy of individuals.

Answers to Questions

1. Clear over-arching principles must be established. The IPC/O believes the following principles form the basis of effective privacy protection on the information highway.

   - *Privacy should be respected and protected.*

     This is because the increasing complexity of the information highway will allow the tracking, combining and analyzing of vast amounts of personal information. This will permit the creation of personal profiles and the monitoring of individuals. To the extent that individuals perceive the threat to privacy as outweighing the benefits, the information and services on the highway will not be used to their full potential.

   - *Before introducing any new technology or service, the impact on privacy should be considered.*

     Privacy concerns should be incorporated into the design and implementation at the outset. It is more costly and difficult to do this once the system is operational.

   - *The collection, retention, use and disclosure of personal information should be governed by fair information practices, established by law.*

     The best known code of fair information practices is contained in the OECD guidelines, which is the basis of Canadian legislation. Although there are a number of industry-specific voluntary codes, in some cases they do not meet the OECD guidelines. This could become a potential barrier to the exchange of information across national and international borders, as well as between the public and private sectors. The best way to avoid this would be by the enactment of federal legislation covering the private sector. This could be complemented by provincial legislation, similar to the Quebec privacy legislation covering the private sector. Such legislation should incorporate standards covering collection, use and disclosure, access and correction, and notification. The purpose of collection should be clearly specified, collection should normally be directly from the

individual, and be made only with the knowledge and consent of the individual. Secondary use and disclosure should only be done with the informed consent of the individual. Also, individuals should have the right of access to and correction of their personal information. Individuals should be notified of the reasons and legal authority for the collection, whether it is mandatory or voluntary, how it is to be used and disclosed, the consequences of providing or withholding the information, and who to contact with questions.

- *Information technologies or services that can threaten privacy should incorporate appropriate privacy protection measures at no cost to the individual.*

  New technologies and services should not diminish privacy. At the minimum, existing levels of privacy should be able to be maintained at no extra cost.

- *Public education and training should be provided about any security/privacy issues surrounding the use of the information highway.*

  Service providers should be responsible for informing the public of any privacy issues pertaining to their services.

- *Personal information should be protected by the implementation of appropriate security safeguards.*

  As a general rule, technical solutions (e.g., passwords and encryption) and security procedures should be proportionate to the risks involved. Consideration should be given to the encryption of sensitive personal information and information at high risk of improper access.

- *A means should be established to handle complaints and to provide redress.*

  To encourage compliance with a common code of fair information practices, an independent means to handle complaints, and where appropriate, to impose penalties and award damages for improper use of personal information, should be established.

2. IPC/O believes that governments, at all levels, should be involved in developing and implementing stronger privacy protection measures. The four approaches outlined in the Discussion Paper can form the basis of these measures.

   As noted above, federal and complementary provincial legislation for the private sector, incorporating provisions for complaints and

redress, is supported. Moreover, the government must play an ongoing role as a regulator, similar to that currently carried by the CRTC. Regulatory bodies should require the submission of privacy impact assessments when new services are introduced. To do so would force the consideration of privacy protection measures early in the design stage and would be cost-effective.

IPC/O encourages voluntary codes as a first step toward data protection in the private sector. However they do not provide comprehensive coverage across the private sector; they may not meet the EC standard of "adequate" privacy protection; they can be difficult to enforce; and, there is often a lack of data subject input and control. Therefore, over the long term, both public and private sector legislation is the most effective.

It is agreed that certain technologies may be used to enhance rather than erode privacy e.g., blind signatures based on a public key system of encryption. New technology also must provide individuals with options to exercise a level of control over their personal information. Moreover, privacy protection must be a key consideration up front, rather than an afterthought. By default, consumers are in a reactive position, which may lead to expensive modifications or complete rejection of a product, as in the case of the "Lotus Marketplace: Households". Therefore, privacy protection should be one of the basic design criteria for technology and services.

There is a fundamental need to educate businesses about privacy implications and to raise the awareness of consumers. All parties should shoulder the responsibility for education. However, public education is not enough. An integrated approach is necessary to ensure that all parties involved in the information highway are equally informed.

3. IPC/O supports an approach that coordinates legislation at all levels. A combination of a legislative framework and sectoral codes, akin to that adopted by New Zealand, could ensure that privacy rights are guaranteed, while permitting a level of flexibility for the unique characteristics of different sectors. Canadian legislation also should be harmonized with international developments because the information highway does not stop at the border.

4. It is important to encourage businesses to see privacy protection as an integral and necessary part of doing business. However, as indicated under Question 2, voluntary privacy codes, as currently implemented, do not provide comprehensive privacy protection.

Therefore, IPC/O only supports voluntary privacy guidelines, developed by business, as a preliminary step toward comprehensive legislation for the private sector.

5. The protection of privacy must not be considered in isolation from other issues. Rather, it must be integrated into the decision making process for the information highway. Moreover, one of the key aspects in moving the highway from the abstract to the concrete will be its social acceptability. Therefore, it must be designed to provide high levels of privacy protection. If privacy protection is integrated into the design process at the earliest stage, it should not slow the pace of development nor unduly raise the cost of innovation. It is recognized that secure systems are generally more expensive than non-secure systems. However, the costs, in terms of human dignity and autonomy, are too great not to require high levels of privacy protection to be built in.

6. Initiatives such as the Discussion Paper, CRTC hearings and the grass roots consultation process of the Coalition for Public Information, all help to involve the public in the policy decisions related to the information highway. However, there has been little consultation with the public in terms of technological developments and practices at a fundamental level, i.e., how will it impact on society, rather than will it be more efficient. Therefore, businesses need to consult with, and listen to, the public when developing products and services that could potentially threaten privacy. This may represent a fundamental, but necessary, change in Canadian business practices.

7. Governments at all levels must make public education a priority and ensure that the necessary funding and resources are made available. Private sector service and information providers also must share in this responsibility. Moreover, Canadians need to take initiatives to become better informed consumers. Also, privacy commissioners and others involved in the development of the information highway must work to protect the public's interests, to raise privacy concerns and foster public debate.

Privacy Commissioner of Canada

The Privacy Commissioner of Canada is the federal privacy ombudsman, appointed by Parliament to investigate complaints about federal government collection, use and disclosure of Canadian's personal information. He also oversees the application of the Privacy Act which embodies internationally accepted codes of fair information practices.

After a comprehensive review of the major issues affecting privacy on the information highway, the Privacy Commissioner concludes that a strong legislative framework (provincially, federally and at the international level) is essential. Voluntary codes, technological solutions and education are all seen to have a place in the privacy equation, however, they cannot alone resolve the complex web of privacy concerns and commercial interests that arise on the information highway.

Personal information is the property of the individual to whom it relates. This basic tenet applies whether information is processed by quill pen or by computer. Moreover, privacy is not just a product of the computer age. Long-standing laws have prohibited electronic eavesdropping and the reading of other people's undelivered mail.

General concern is expressed that, in some quarters, the speed and convenience of the information highway warrants some sacrifice of privacy. This proposition is not accepted, even though there may be some difficulties in protecting personal information on the highway. To do otherwise, may cause the public to avoid full utilization of the highway, to the detriment of increased government efficiency and private sector competitiveness. Specific concern also is expressed about the privacy rights of individuals who use E mail. In the absence of specific consent, E mail is regarded as a private communication. Attempts should be made to protect E mail from interception. However, where this is impossible, users should be informed that their E mail is not secure. In addition, concern is expressed about the vulnerability of specific types of information, namely, health information and transactional information. Health information is particularly sensitive and requires additional protective measures. Transactional information can leave a data trail which may say something about a person's beliefs, tastes or financial and credit situation. Therefore it needs protection. Monitoring and surveillance of mobile telephone users, by the use of geo-positioning satellites, also is seen as a concern. The use of such technology, often known as the "electronic leash", represents a convenience. However, in the absence of legal authority to do so, information acquired should only be used to facilitate the technical communications link.

The federal Privacy Act and equivalent provincial legislation have generally not addressed privacy protection in the private sector, with the sole exception of Quebec. However, on the international scene, this has been done by the OECD guidelines.

The following principles should be incorporated in legislation for both the public and private sectors.

- The collection of personal information should be limited to the details necessary to provide the good or service.

- Carriers and controllers should be required to explain their data protection practices and the privacy implications of new technology to clients.
- Individuals must be given control over their personal information transmitted on the information highway.
- Disclosure of personal information, without the individual's explicit consent, should be prohibited.
- Individuals should be provided with access to their personal information, and carriers and controllers should ensure that it is accurate and up-to-date.
- Charging for privacy should be prohibited.
- An independent oversight mechanism to monitor privacy protection and to provide a means of redress should be established.

The distinction between the public and private sectors is becoming more and more blurred through processes such as contracting out and using private carriers to transact government business.

There should be consistency of privacy legislation at the federal and provincial levels. Otherwise, attempts could be made to evade privacy protection measures by setting up business in the most lenient jurisdiction. This could cause some jurisdictions to lose business to less stringent jurisdictions. Moreover, it could lead to the need to develop artificial legal distinctions about where data is "located".

The protection of privacy cannot be left to the whims of the marketplace. Therefore, the federal government should enact legislation to protect privacy on the information highway in both the public and private sectors, and should encourage provinces to enact complementary legislation. It should be based on fair information practices and on the principles outlined above, and provide appropriate sanctions.

Voluntary codes cannot provide adequate levels of protection. Voluntary means just that - unenforceable and apt to be ignored by those who have a financial interest or competitive advantage to gain. They are like a chain, only as good as the weakest link. Moreover, they can leave individuals with no enforceable rights, and are often only half measures. However, voluntary codes have a place in the overall picture. They can serve an educational purpose

Technological solutions also have a place but cannot stand alone. In this regard, security of information is an important aspect, and the development of effective encryption and secure transmission facilities have an important role. However, encryption raises an important issue - should it be permitted to be so effective that it cannot be broken by law enforcement agencies?

Although carriers have a responsibility to ensure that their transmission lines are basically secure, they cannot be held responsible for the privacy protection of the actual information carried on those lines. In fact, they should have a positive obligation not to examine the information they are carrying. Security of the information itself is the responsibility of the information controller. This may involve encryption of sensitive personal information, such as medical information. Where such security cannot be assured, there should be a positive obligation to inform the subject of the lack of security. Furthermore, privacy considerations should be incorporated in the design of new technologies. This should be aided by privacy impact assessments that would be available to regulators and the public.

Similarly, education also has an important role to play. Consumers should be informed about the impact of new technologies on their privacy and how it may be protected. Equally important, is the need to educate people about the ethics of acquiring and handling personal information. In this regard, the Privacy Commissioner and his provincial counterparts can play an important role. Service providers also have an equal obligation. In this way, consumers can be free to choose whether to use the services being provided and the level of security they require.

British Columbia Government

This submission is made on behalf of the Govemment of British Columbia by the BC Ministry of Employment and Investment.

The province concludes that a consultative process should occur between all levels of government regarding the appropriate legislative/regulatory role that governments should play in protecting individual privacy. This should also involve the private, educational and general public sectors. However, reliance on self-regulation must be balanced with the need, where necessary, of govemment to act in regulating activities.

The Province recognizes the tremendous potential offered by the information highway. However, with advances in information transfer, collection and handling technology, the potential threat to individual privacy increases. Problems associated with data matching, transactional data, network security, and general dissemination of data are increasing. To meet these concerns, appropriate privacy protection measures should be implemented quickly in Canada.

Answers to Questions

1. The province supports the Federal Government Telecommunications Privacy principles. In addition, it supports the descriptive components of the right to privacy enunciated by its Information and Privacy Commissioner as follows.

   - The right to individual autonomy.
   - The right to be left alone.
   - The right to a private life.
   - The right to control information about oneself.
   - The right to limit accessibility.
   - The right to minimize intrusiveness.
   - The right to expect confidentiality.
   - The right to enjoy solitude.

   Also, privacy decisions should be based on the principle that holders of individuals' personal information have power over those individuals, that use of that information may cause harm and, therefore, that information must be used responsibly.

2. Legislation at both the provincial and federal level is necessary to ensure privacy protection of government held personal information. Such legislation should incorporate all of the 12 primary data protection principles and practices contained in the submission of the Information and Privacy Commissioner of British Columbia. As well, it should provide for personal consent to collection and disclosure, disclosure of what types of information is held, a right of access, and a positive obligation to ensure that appropriate security measures are implemented.

   The question of private sector legislation should be considered by all jurisdictions on its merits. If such legislation is enacted, it should be coordinated between jurisdictions, otherwise there will be problems with inter-provincial and federal-provincial transfers of information.

   Prior to the passage of legislation, an effort should be made to get industry to adopt privacy codes. Self-regulation, if successful, is more efficient and economical. Moreover, codes could be effective where there is a central accrediting or licensing body. Although industry privacy codes are more flexible, a national standard upon which industry codes could be modelled would help to ensure a common and comprehensive approach. Therefore, the Province supports the development of the CSA's privacy code.

   Technological advances can benefit privacy as much as they can threaten it. The use of security access codes and encryption are important tools.

5. The issue of privacy is too important to be neglected in favour of unchecked development.

6. Governments should adhere to general principles of consultation in the design stages of systems which they will use. Where the privacy threat is great, there should be a consultation process similar to other regulatory consultation processes.

7. All sectors should have a role in educating the public regarding privacy issues. Regulatory bodies, such as the CRTC, various consumer and corporate branches of government, as well as information and privacy commissioners, all can become involved. In the case of the latter, education should become an element of their mandate. This function also can be carried by consumer groups, educational institutions, and the private sector.

Health and Welfare Canada

The submission discusses the overall concept of privacy and confidentiality and its various consequences, the administrative and statistical uses of data, privacy of medical records, and voluntary codes and standards, all as seen from the standpoint of Canada's national health authority.

The Discussion Paper's definition of privacy could be open to some misinterpretation. Privacy is a basic human right but it is not an absolute right. The rights of society in general also need to be factored in. Also, the question of "rights" can become very emotional. Therefore, confidentiality and the importance of making organizations accountable for personal information under their control are seen as the critical issues.

Strong concern is expressed that a distinction be made between the use of personal information for administrative purposes (the information will be used in a "decision making" process that directly affects the individual) and its use for statistical and research purposes. In cases where confidentiality is paramount and protection measures are completely adequate, use for legitimate research and statistical purposes should not be restricted. This is very important if new knowledge is to be gained on diseases and health risks at the national and international level. Moreover, it is believed that the public is well aware of the importance of research in these areas.

The privacy of medical records is a most important issue. Although the issue appears well covered in the federal Privacy Act, health care is a provincial responsibility and not all provinces have privacy legislation. Moreover, health records also are held by the private sector which is virtually unregulated and this may lead to potential abuse. There are several possible solutions. One is the development of uniform provincial data protection laws that would apply to the complete health sector and other users of health care information. Models of such legislation are the UK Data Protection Act and the US Uniform Health Care Information Act. Another is the development of model codes for the protection of health care information. These already exist in a number of domains and, although lacking the force of law, their importance should not be discounted.

HWC supports the intent and purpose of voluntary privacy codes, particularly the CSA draft model code. However, some of the principles contained in the CSA code cause concern.. The principles relate to "consent", "identifying purpose" and "limiting use, disclosure and retention". A literal enforcement of these principles could serious inhibit or curtail legitimate research activities. In the epidemiological and other medical research fields, large volumes of personal data are required for statistical data matching, and this precludes strict compliance with the principles noted above. However, health researchers and research organizations, such as the Medical Research Council and the Canadian Institute of Health Information, have adopted principles based on the OECD guidelines,

developed policies to protect the confidentiality of individual records, and developed procedures to protect against the inadvertent disclosure of small cell data.

Prince Edward Island Department of Health and Social Services

Concern is expressed that privacy legislation could impede pharmacoepidemiology research. It is important that there be provision for the carrying out of these studies using anonymous information which is kept confidential. There must be recognition both of the privacy issue and the need to obtain health research information.

Saskatchewan Provincial Secretary

This submission is made on behalf of the Telecommunications and Broadcasting Policy Unit of the Saskatchewan Provincial Secretary. It does not represent the views of the Government of Saskatchewan.

It is crucial that privacy issues be seen as important to the growth and development of the information highway. In their absence, users will not incorporate the highway into their daily routine.

Saskatchewan will be pleased to consult on any proposals and recommendations stemming from the deliberations of the Advisory Council.

Canadian Labour Congress

In summary, legislation is seen as essential because voluntary codes have proven themselves to be inadequate. The common private sector definition of privacy is disputed and numerous concerns are expressed. A number of principles to form the basis of effective privacy protection also are provided.

Public and commercial interests tend to define privacy as confidentiality. This ignores the basic precept of the ability to exercise control over personal information.

Numerous concerns are expressed over privacy invasions which could occur due to the vast amounts of personal information held by governments, employers and the private sector. The transfer of personal information, as a result of public-private partnerships, as well as its transfer abroad, also are matters of concern.

Comprehensive legislation must include the following principles.

- Individuals must have control over their personal information.
- Information should go only when and where it is intended.
- Collection should be limited only to the details essential to provide a service.
- Disclosure should be prohibited without explicit consent.
- Data collection procedures must be clearly explained to customers.
- The use of records that show how and when an individual used the highway must be prohibited, in the absence of informed consent.
- The use of transactional records must be restricted to consented and lawful purposes.
- Appropriate cryptography and other technical security measures to protect the privacy of electronic communications should be mandated.
- Charges or fees for privacy protection must be banned.
- Government must monitor privacy protection on the highway.
- A fair information practices code to govern the highway should be legislated.
- Stringent penalties to discourage violation must be included.

Broad privacy legislation for business, government and the non-government sector is deemed to be essential. It should be based on the foregoing principles, and provide a framework for all concerned. With the exception of

Quebec, which has established a model of private sector privacy legislation, Canada is seen as one of the only countries in the advanced industrial world that does not provide adequate protection of personal data held by the private sector. Legislation must ensure that all users of personal information are bound by the same guidelines.

The patchwork of voluntary privacy codes has proven to be wholly inadequate, particularly because, in many cases, they do not provide independent arbitration for complaints, and they serve business interests rather than those of the consumer. Moreover, the Telecommunications Privacy Protection Agency was never activated. The CSA draft model privacy code shows promise, if it can overcome the invasive capabilities and the pace of technological change.

Canadian Standards Association (CSA)

The ten principles outlined in the CSA Model Code for the Protection of Personal Information are supported as the basis for effective privacy protection. Technological solutions and consumer education also have a part to play.

The CSA code has been drafted on the basis of consensus. Voluntary codes will enhance the effectiveness of the other three approaches outlined in the Discussion Paper. Moreover, they may use other methods than law to ensure compliance. During 1995, CSA will be studying options for the implementation of its own code. Furthermore, they are often good for business, e.g., by improving the quality of information management.

The information highway will need privacy protection. At the very least, the system needs to minimize the vulnerabilities of E-mail and fax and provide for encryption. CSA is already involved with information technology standards, including those on security devices and smart cards.

There is no doubt that consumer privacy education is needed. This responsibility should be shared by all information gatherers. The publication of the CSA code is seen as a means of increasing consumer awareness.

Specific Proposals and Recommendations

As a consensus facilitator, CSA would be prepared to assist in the consumer education process.

COMSEC Services Inc.

COMSEC Services is a company engaged in communications security.

This submission deals mainly with technical security on the information highway. A parallel is seen between the privacy intrusions of scanners on cellular telephones and similar potential intrusions on the information highway because of inadequate security standards adopted for current telephone circuits. Potential breaches of information security on the highway must be addressed by the Advisory Council and, if a breach occurs, the carrier should notify the subscriber of the breach or, at the very least, notify subscribers of technical standards weaknesses and ease of compromise.

Bill Doskoch

Bill Doskoch is a journalist in Regina. He is a member of the Canadian Association of Journalists and a co-founder of its Computer-Assisted Reporting Network. However, his response is being made solely as a private citizen.

The need to balance the protection of privacy against the importance of maintaining open government and the freedom of expression provisions of the Charter of Rights and Freedoms is seen as essential. Restriction of access to government information because of privacy laws is feared, however this restriction need not occur if information is anonymized. Nevertheless, provision must be made for the release of personal information when it is in the public interest to do so.

It also is suggested that media databases which are marketed to the public and which contain personal information should be subject to fair information practices. However, this raises other problems such as the verification of the fairness and accuracy of such information, and the possible need to establish hypertext links between letters to the editor and any correction or clarification connected to a particular story.

Eridani Productions Ltd.

The writer, Robin Rowland, is a freelance writer and television producer. He will be teaching Canada's first Computer Assisted Reporting course at Ryerson Polytechnic University, Toronto.

The Advisory Council is urged to bring in a report that balances the need for privacy with a strong recommendation for an open records law. This view is based on experience with Computer Assisted Reporting which uses database and spreadsheet software to find the story behind the story. Examples are presented on how this method has been successfully used in the USA to uncover election frauds, dangerous or impaired driving records of school bus drivers, etc. Many other similar stories are pointed to in a book entitled "Investigative Reporters and Editors: 101 Computer Assisted Stories from the IRE Morgue". Because it is essential that government

information be open to the public, and to the news media in particular, concern also is expressed that privacy measures could be used to restrict access to large numbers of records, even though in most cases personal information could be deleted.

Curtis E.A. Karnow

Curtis Karnow is a lawyer with the firm of Landels, Ripley & Diamond of California. He specializes in computer technology and related legal issues. His articles have been published in a wide variety of journals and he includes a copy of a speech which he gave in London which alludes to the global nature of the issue.

It is submitted that personal information is the property of an identifiable individual, subject only to specific exceptions, e.g., the press which should not be shackled by concepts of ownership and property if information is anonymous.

A fundamental principle is that data collected by one entity for one purpose should not be used for another purpose or by another entity, in the absence of express permission.

He strongly endorses the concept that lawmaking, including the absolute guarantee of privacy, must be established at the federal level in Canada, because privacy rights are both national and international. However, caution is expressed that detailed legislative schemes will be outdated before they can be put into effect. Rather, the emphasis of legislation should be on propositions such as the articulation of fundamental privacy and the ownership of data. Moreover, the government should establish privacy as a Charter right.

It is not believed that the government, or any other group, can design an information highway because it evolves. The government can only provide the right conditions, including freedom of speech, access to powerful encryption, deletion of restrictions on development, and a forum for those injured on the highway to have redress. Moreover, because the electronic world is not limited to any province, state or country, it is useless for the government to try to restrict the dissemination of information in or out of Canada, because any legislative efforts would only be overridden by technological development elsewhere in the world. In regard to encryption, the government must allow and encourage the free availability of strong encryption software without any restrictions on its import or export.

Veronica Lacey

Ms. Lacey is the Chair of the Working Group on Learning and Training of the Information Highway Advisory Council.

Concern is expressed about the numerous types of privacy invasions that can occur by the unauthorized use of and access to educational records. Learning records, student freedoms, individual stalking, multimedia courseware transactional records, teacher training, fraud, and federal/provincial cooperation are all singled out as requiring special attention. A balance must be achieved between use and access essential to fairly administer educational programs and use and access that may be detrimental to an individual's legitimate privacy rights.

Specific Proposals and Recommendations

- Learning records should be encrypted and shared only with consent.
- Also, creation of cradle-to-grave records must be guarded against.
- Learning and training records transmitted on the information highway should be encrypted.
- Transactional records related to learning and training should remain anonymous and unavailable to any viewer outside of the educational and training systems.
- Teacher training courses should include privacy awareness and study.
- Federal/provincial discussions will be required to determine how best to protect sensitive learning and training data on the highway.
- Representatives of the learning and training communities should join the CSA Privacy Committee to provide an educational perspective in the development and implementation of privacy standards.

Detective Superintendent Ken Grange

Det. Supt. Grange is with the Metropolitan Police Service, New Scotland Yard in London, England. He has been involved in privacy issues related to police work.

The submission is presented as the personal views of a police officer engaged in the fields of data protection and academic research. It concentrates on the problems and shortfalls of the UK Data Protection Act, 1984, which might be kept in mind when considering the direction to be taken in Canada. Also, it suggests that stronger measures are required to protect the privacy and security of personal information by a combination of legislation, voluntary codes, technological solutions and education.

The UK Data Protection Act is seen as having a number of practical and operational problems. Under the UK Act, the data registration process is entirely too bureaucratic, is ignored by the vast majority, and takes up too much time of the Office of the Data Protection Registrar. Therefore, any

data registration should be limited to defined sensitive data, thereby allowing the Office to deal only with complaints in regard to sensitive data and other more serious breaches of the Act.

The right of access by individuals is seen as an area of serious abuse. Ninety percent of all access applications to the Metropolitan Police are the result of consent being forced on current or potential employees by employers. This subverts the principles of the Act and circumnavigates the workings of the Rehabilitation of Offenders Act.

The principle of consent to collection and disclosure sometimes causes problems because the UK Act has no provision for public interest exemptions when data collected for one purpose is used for another. This can be a particular problem, following commission of a crime, in regard to disclosure to victim support agencies, local authorities, social services, etc. Also, many other organizations have investigative functions and may have legitimate reasons to be provided with personal data. Thus, in a time of severely restricted police resources, this could lead to the inability of industry to deal effectively with cases of fraud.

In the UK Act, the principle of the protection of the security of data is rather vague. Thus, the problem of "hacking" is not mentioned. This was not dealt with until the specific Computer Misuse Act of 1990. Accordingly, legislative provisions to deal with the technology itself are not effective to deal with problems in the short term because of the rapidly evolving nature of technology.

Approaches

I. Any legislation should aim at a level playing field across Canada in terms of achieving common standards, because this is a continuing problem in the European Community. The legislation should be aimed at the protection of data and not at the technology or network infrastructure. To do so would render the legislation unworkable and unacceptable to both the public and private sectors, and would place Canada at a commercial disadvantage in a competitive world. Moreover, such legislation could moderate the clear benefits which technology brings to the public.

II. A voluntary codes and standards approach could provide the opportunity for sectoral groups to build on the broad principles contained in legislation, as is the case in the UK legislation. Under the UK legislation, the policing sector agrees its internal codes with the Data Registrar and, if it contravenes those codes, it is subject to sanctions and enforcement by the Registrar.

III. Technological solutions are seen as having considerable merit. Although legislation should not stand in the way of technology in

attempting to protect privacy, the technology can go a long way to protecting privacy. Therefore, the technology industry should be persuaded to develop technical solutions to privacy problems, thus increasing the commercial viability of those systems.

IV. In the UK, individuals are perceived as largely ambivalent to data protection issues unless they are directly affected by a breach or by inaccurate data about themselves. The low rate of requests for access to personal data is seen as evidence of this. Even so, education is recognized as an area where a lot of impact can be made through, perhaps, the inclusion of privacy protection in some form of customer or citizens' charter.

Answers to Questions

2. Stronger measures are seen to be needed but they must be realistic and achievable. The experiences in the UK are thought to be a good indication of both how and how not to proceed. A combination of the four approaches (legislation, voluntary codes, technological solutions and education) is deemed to be the proper way ahead.

Specific Proposals and Recommendations

Any legislation should proscribe the use of enforced consent to obtain access to an individual's personal information.

CANADIAN STANDARDS ASSOCIATION (CSA)
DRAFT MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION

PRINCIPLES IN SUMMARY

1. Accountability

An organization is responsible for personal information under its control and shall designate a person who is accountable for the organization's compliance with the following principles.

2. 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.

3. Consent

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

4. 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.

5. Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

6. 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.

7. *Safeguards*

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

8. *Openness*

An organization shall make readily available to individuals specific information about its policies and practices relating to its handling of personal information.

9. *Individual Access*

Upon request, an individual shall be informed of the existence, use and disclosure of personal information about the individual 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.

10. *Challenging Compliance*

An individual shall be able to challenge compliance with the above principles with the person who is accountable within the organization.