Draft

CONSUMER POLICY ISSUES IN THE PRIVACY OF PERSONAL INFORMATION

Consumer Policy Branch
Consumer and Corporate Affairs Canada
November 25, 1992

This paper presents the views of its author and does not represent the opinions of Consumer and Corporate Affairs Canada or the Government of Canada.

TABLE OF CONTENTS

INTRODUCTION

The purpose of this paper is to examine privacy issues affecting consumers that also have policy implications for federal and provincial governments and for the private sector. In examining the issues, the paper will provide a brief overview of the history of privacy values and issues. Two multilateral initiatives, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the draft EC Directive on Privacy are reviewed for their implications for Canadian policy. Finally, this paper will analyze the response of business to current federal government policy on privacy and, for the purposes of federal/provincial discussion, recommend possible policy directions affecting the consumer interest.

For the purpose of this paper, privacy refers to the privacy of individuals with respect to personal information and data about themselves held by private organizations in the marketplace.[1] The term data protection, which is also used throughout, has its origins in European privacy protection legislation. The term connotes the impact of computer and word processing technology since the late 1960's and distinguishes this from the broader generic concept of privacy, which has a strong tradition and important place in liberal democratic heritage.[2]

THE ISSUES

Privacy experts understand there is to be at least four major issues related to the use of personal information in market economies which are of concern to consumers.[3] These issues are:

- the indiscriminate collection of personal information, often as a condition of a transaction or as an inducement to establish a relationship with business (contests, warranty information) when some of the information may be superfluous and intended for a separate and unstated purpose;
- the general absence of reasonable standards for the accuracy and security of personal information;
- the general inability of consumers to access information held about them for verification of its accuracy, or, on the other hand, the imposition of a fee to access information held about them; and

---

[1]David H. Flaherty, Protecting Privacy in Surveillance Societies, University of North Carolina Press (Chapel Hill: 1989), p. 253.

[2]Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press, (Ithaca, New York, 1992), pp.12-17.

[3]Privacy issues and principles of data protection are recognized by experts as two sides of the same coin (See Colin J. Bennett). The number of issues/principles highlighted in any one discussion may vary according to the specificity with which analysts wish to treat the subject as well as the nature of the application that is under discussion. For ease of discussion, CCAC has chosen to condense the issues to four, accepting that our analysis acknowledges a greater number of principles of data protection.

- the possible use/disclosure of personal information to third parties without the knowledge or consent of individual consumers.

BACKGROUND

Canadians are constantly under surveillance, not necessarily visually, but informationally. Each time we make a purchase with a credit card, make a withdrawal from the bank, make a telephone call, subscribe to magazines or catalogues, we leave a data trail. The number of goods and services linked to data trails and data capture is proliferating. Consumers are, in many cases, unaware of the scope of the surveillance. In other cases, society appears to accept the casual existence of unknown numbers of individual files with little or no concern for the accuracy of the information until issues affecting large numbers of consumers elicit a strong public reaction.[4]

The development of electronic information storage, processing and retrieval technology over the last few decades has encouraged businesses to collect, for their own benefit, detailed personal information about individuals. Today's technology has become manageable to the point that data can be collected and matched from various sources and merged to produce detailed profiles of individuals for a variety of purposes. Personal information has become a valuable resource that acquires increasing value through storage, processing, reproduction and distribution.[5] It has become a commodity in its own right for both business and government. The implications of this are profound for both consumers and data collectors. John Grace, former Privacy Commissioner, commented:

> Wonderful as the possibilities are, the new technology, without ethical constraints, could turn ours into a watched society in a way that George Orwell never imagined...The computer transcends time and space by mining our information, interrelating programs and actions, and producing chillingly accurate profiles. An individual's right to be left alone, to control what the rest of the world knows about him or her, is profoundly diminished.[6]

The result of these developments is that much is likely known about us by more people than we are aware of and may be comfortable with. Given the likelihood of continuing technological evolution, experts seem to share the view that privacy issues are not temporary phenomena and will not fade with time.[7] They are likely to intensify in the years ahead, raising questions in North America about the role of governments in their resolution.

---

[4]Privacy Commissioner - Annual Report, 1991-92.

[5]Vanda Rideout, The Implications of Information Technology on Personal Privacy, a report prepared for the Strategic Planning Division, Research and Spectrum Sector, Department of Communications, 1992, p. 3.

[6]John Grace, "The Ethics of Information Management", Canadian Public Administration / Administration Publique Du Canada. V. 34, No. 1 (Springtime/Printemps), p. 96.

[7]James E. Katz, "Public Policy Origins of Telecommunications Privacy and the Emerging issues" Privacy Vol. 10, No. 3., July 1988., p. 173.

Historical Perspective

Privacy values in western societies have their roots in the late seventeenth century.[8] Political philosophers, such as John Locke, and later, John Stuart Mill and James Madison, advocated the recognition and the preservation of the rights of the individual. The gradual move towards individualism in subsequent centuries provided the philosophical underpinning of today's privacy values.

In North America, individualism gave rise to an intellectual tradition that valued the privacy of information about individuals and about private businesses. This tradition is reflected in the general principle that record-keeping by business and decisions about the use of such records is, generally, a matter for decision by individual companies and not by governments. Thus, supply-side considerations (the expansion of markets), rather than social policy concerns, have traditionally formed the basis for approaches to the privacy of personal information held by businesses in Canada and the United States. To date, governments have tended to leave the responsibility for privacy protection in the private sector to voluntary initiatives by the private sector.

Today, the application of technology and the continuing emphasis on individualism has created a conflict between the consumer's right to privacy in the marketplace, based on historic practice, with the perceived contemporary right of business to gather and use personal information. It is possible to conclude that protection of society's privacy rights has failed to keep pace with the acceleration of technological development, although Canada's Privacy Act and Access to Information Act and similar legislation in Québec, Ontario, Saskatchewan and British Columbia have tried to narrow the gap, at least with respect to personal information held in the public sector.

Consumer Behaviour and Attitudes

Consumers usually volunteer personal information to businesses in order to receive goods and services. The tacit, if naive, understanding among consumers has been that the business collects only that information necessary for the provision of the goods and services being sought by the consumer and that the information will only be used for the purpose for which it was collected, unless the consumer is asked and consents to alternative uses. However, there is evidence of the growing collection and use of personal data which has led to the actual misuse of personal information. There is also a growing perception that once we enter the marketplace, we begin to give up our privacy.[9] Anecdotally, changing consumer interest is reflected in the growing number of complaints to government departments and regulatory agencies about aspects of privacy, both intrusion (junk mail, list sales, phone solicitation and the use of social insurance numbers) as well as control of the flow of personal information (how did they get my name?). The level of misuse may be

---

[8]Ibid., p.169.

[9]James E. Katz and Annette R. Tassone, "Public Opinion Trends: Privacy and Information Technology", Public Opinion Quarterly, Vol. 54, No. 1, Spring 1990, p. 128.

controlled somewhat by allowing consumers to access files containing personal information held by the private sector to determine its origin, ensure that the data is accurate, complete and up-to-date, as well as requiring appropriate security measures be taken to protect data from unlawful or accidental access, alteration or destruction. This could minimize the use of tenant, employee and insurance blacklists, for example. However, this can affect consumer behaviour only to the extent that consumers are aware of the existence of data held about them.

Some consumers and consumer organizations appear to be taking matters into their own hands by providing or recommending the provision of only that information that is relevant. There is some indication that this may also involve the provision of misinformation such as bogus telephone numbers and addresses so as to appear to satisfy the information requirements of a transaction. This also serves as an outlet for those who are frustrated by the amount of information that is asked for.

In the contemporary environment, conflicts concerning the right of individuals to determine who can have access to personal information about them, what information third parties should have access to, and what the information should be used for stem, in part, from perceptions about the ownership of personal information. It is possible for consumers to claim that they have ownership of their personal health and medical information, financial data, and credit information, and therefore they can exert control over its collection and dissemination by second parties.[10] However, a voluntary disclosure of personal data to businesses or to other third parties, such as doctors, in return for goods and services may represent a transfer or a sharing of ownership. In contrast, the private sector claims ownership of the information that it collects, stores, processes and generates and that ownership supersedes individual rights. In some cases, such as aspects of financial or other services, a duty of care may exist on the part of the party that has received the information.[11] In the case of most marketplace transactions however, no such duty has been voluntarily established nor is there relevant legal precedent.

In Canada, it is difficult to gauge the extent to which consumers are aware of or concerned about personal data collection. There has been little significant public reaction and little publicity. Furthermore, until very recently, significant national public opinion research has not been conducted in Canada on the general issue of privacy, and public

---

[10]James L. Brown, "Consumers, Cards and Controls: Privacy in the World of Electronic Financial Services", a paper prepared for the Third International Symposium on the Consumer and Financial Services, April, 1992, p. 12.

[11]Privacy Times, Vol. 12, No. 13, July 1, 1992. p. 4. This article describes a recent Supreme Court decision concerning a doctor's refusal to disclose to a patient information obtained about her from other physicians. The court determined that patients have a right to see their files because their special relationship with the physician creates a fiduciary interest in the data. McInerey V. McDonald, June 11, 1992.

attitudes, values and experience are difficult to gauge.[12] However, a recent major survey conducted in the United States shows that 79 percent of Americans are concerned about privacy and 71 percent feel that they have lost control over how personal information about them is circulated by companies.[13] In jurisdictions where public opinion research has been conducted, analysis shows that personal privacy, and data protection in particular, are consistently of concern to respondents among all classes, ages, genders and races. The concern is over three aspects of privacy; as an aspect of human dignity, its political implications (personal information in the hands of perceived powerful governments) and reservations about the use and disclosure of information held in computers. Canada is unlikely to be an exception to this pattern. While this suggests a broad awareness and concern about personal data protection, it should be recognized that as a societal issue, its importance has been superseded in public opinion research if tested in comparison to other major issues such as the impact of crime and unemployment and the threat of war.[14],[15]

Consumer concern over the privacy issue is in part manifested by the growing activity of consumer advocacy and public interest groups. Such groups as the Consumers' Association of Canada (CAC), the Service d'aide au consommateur - Shawinigan (SAC)[16], the Public Interest Advocacy Centre (PIAC)[17], and the Québec Human Rights League[18], are participating in the privacy debate. The general consensus among these groups is that government should regulate, at least to some degree, in this area.

---

[12]Various government and private sector organizations, including Stentor, Bell, Canadian Bankers Association, AMEX, Bank of Canada, Equifax Canada, Statistics Canada, Communications Canada and Consumer and Corporate Affairs Canada are currently developing a national privacy survey scheduled to be completed by early 1993. This will provide, for the first time, substantial information for government and private sector policy-makers on privacy issues.

[13]Harris-Equifax 1991 Consumer Privacy Survey, p. 3.

[14]James E. Katz and Annette R. Tassone, "Public Opinion Trends: Privacy and Information Technology" Public Opinion Quarterly V. 54, No. 1, Spring 1990, p. 126.

[15]It should be noted that public opinion surveys about privacy conducted by telephone can generate downward-biased results. This arises because those most concerned with privacy rights will likely not respond to a survey on privacy, since a survey itself may represent an invasion of privacy. Thus survey results may be underestimated. This is discussed in: Katz and Tassone (1990).

[16]The SAC published a report entitled Le Dossier Noir de la Vie Privée (March 1992), which provides analysis of the current Canadian and international situation, and makes recommendations on courses of action.

[17]PIAC received a contribution from CCAC to conduct a study on privacy with the intent of making recommendations. The report has not yet been completed.

[18]The Québec Human Rights League has been active in privacy advocacy. The League's spokesman, Pierrot Péladeau, has represented the organization in a variety of initiatives and workshops, including the Canadian Standards Association initiative, and a recent seminar on privacy in the telecommunications industry.

Legal Parameters

The concept of privacy as a perceived inherent right is by nature complex. In a legal context, privacy can be desegregated into three general categories: territorial privacy, privacy of the person, and intellectual privacy.[19] Territorial privacy refers to property and the freedom of the individual to use it in any way he or she desires. This freedom, however, carries some restrictions insofar as the use of property cannot infringe on the rights of others in society. Privacy of the person maintains that the violation of the physical space surrounding a person is an invasion of privacy. These two categories are relatively well defined and protected under common law and contravention of these rights is actionable under the torts of trespass and nuisance.

Intellectual privacy, the category under which the protection of personal information freedom falls, is less well defined and as such, is less well established in our legal system. While individuals do hold some claim to the use of information held about them, they must balance through choice, their desire for privacy with their desire to participate in the marketplace.[20] In many instances, the consumer may lose the freedom to independently choose to forego privacy because personal information is being collected, used or circulated without the knowledge or consent of the individual. Freedom of choice is also infringed when the consumer must provide personal information as a condition of sale of essential goods and services. There is some statutory protection for intellectual privacy, such as credit disclosure legislation, and there is common-law privacy protection, especially in the tort of breach of confidence. However, there is no integrated set of laws to protect individuals from the creation of personal information files[21] and most areas are not significantly covered by law. Québec, however, may be the first province to introduce legislation regulating the collection and use of personal data in the private sector. This could occur in late 1992, with public hearings as part of the process. The Québec initiative follows on the numerous initiatives in the Europe Community where the latter is adopting legislation and where most national governments have data protection legislation in place.

Economic Parameters

The humanistic, political and legal dimensions of the privacy of personal information are widely identified. It can be argued that data protection is a strictly humanistic concept and is derivative of the broader ideas of personal rights and individual liberty. This argument considers privacy to be a social value that has no intrinsic economic value. In this sense it is a means to an end — that is protecting one's personal authority or one's core self.

The economic dimensions of privacy are less widely discussed and understood. A counter argument to the humanistic concept is that the privacy of personal information exists

---

[19]New Brunswick Government "Privacy and the Canadian Consumer", a discussion paper prepared for the Federal/Provincial/ Territorial Meeting of Ministers of Consumer and Corporate Affairs. 1990.

[20]Alan F. Westin, Privacy and Freedom. New York: Athenaeum, 1979, p. 3. Also, James L. Brown *Op cit*

[21]Cordell in Rideout, *Op cit*, p. 4

as a means to an end other than in itself, namely to ensure that in the marketplace the "...right people use the right data for the right purpose". The right data will be those which are accurate, complete, relevant and timely; the right purposes will be those to which the data subject expressly or impliedly agreed or which are sanctioned by law; the right people will be those who need to use the data for those purposes alone. When any one of these conditions is absent, critical rights, interests and services may be jeopardized[22] at some cost to the individual. This is an efficiency argument implying that in the absence of these conditions, other burdens are transferred to the individual. For example, consumers might have to bear the cost of legal action to protect themselves. Costs can also be passed to society such as those associated with the operation of the court system as a forum for settling privacy disputes. This could arise when, for example, information, which is transient, becomes incomplete or outdated or both. If it was originally intended for direct marketing purposes but is used as a screening device by business, economic hardship can be inflicted on individual consumers. **A policy question concerns the degree to which consumers should have access to any files containing personal information to verify its accuracy, currency, and completeness.**

Yet another argument and an interesting consideration associated with the question of the ownership of personal information is the possibility of personal information becoming a true commodity whereby consumers sell personal data to interested parties for a benefit. This idea possesses some interesting economic, social and legal implications. First, such a development would lead to increased efficiency in the collection, use and disclosure of information by business, and it would help quantify the value consumers place on personal data. Further, the consumer, by being able to choose to sell personal information, is given control over its collection and use. It would also establish a legal foundation against it being collected or misused. Anyone found possessing personal information without a contract having been negotiated, could be charged with theft. Misuse could be actionable under contract law.

---

[22]See Bennett, *Op cit*, p. 33 for a discussion of economic considerations.

SECTORAL ISSUES

Financial services sector

The financial services sector has presented major consumer protection challenges over the past two decades with respect to credit and related disclosure. A new challenge has arisen with the size, scale and proliferation of data processing technology, as well as telecommunications technology, which is creating a new financial services marketplace. The convergence of these technologies has created the convenience and efficiency of electronic banking systems and a range of new products. However, the application of this technology has also given rise to concerns about the capacity of existing consumer protection legislation, which is applicable largely to paper-based transactions, to address the protection of personal data.

A second factor contributing to concerns about privacy in the financial services sector are the recent amendments to various statutes affecting the industry.[23] These new amendments allow for a greater degree of horizontal integration within the industry. It is possible for companies to transfer personal information to affiliated institutions without the knowledge or consent of individual consumers.

Electronic Banking

Each time a consumer makes an electronic banking transaction, the details of that transaction are stored electronically and can be directly attributed to the individual. Transactional information is commonly grouped into some specific categories such as deposits, withdrawals, payments, credits and debits. Thus, the standardized form of financial data associated with new data processing technology facilitates its storage, manipulation and accessibility.[24] Large amounts of detailed personal data are available for surveillance purposes as documented in a submission by Canada to the OECD Committee on Consumer Policy.[25] **The policy question is what limits might be appropriate to the gathering and circulation of such information.**

The enabling characteristics of electronic banking technologies affecting privacy are that:

- financial data is highly centralized and maintained in an electronically readable form, therefore it is more easily and cost-effectively retrieved;
- it is feasible for parties who have legitimate access to the data to use the

---

[23]The Bank Act; the Insurance Companies Act; the Trust and Loan Companies Act; and the Cooperative Credit Associations Act.

[24]James L. Brown, *Op Cit* p. 4.

[25]"Electronic Funds Transfer Systems: An Overview of the Privacy Issue", a paper submitted in 1985 by Consumer and Corporate Affairs Canada to the Chairman of the OECD Working Party on Consumers and Banking, p. 5.

information for a greater range of purposes;

- monitoring improper release is more difficult because of the volume and speed with which information is processed and because monitoring itself may violate systems security procedures. (This latter phenomenon is the focus of some debate between privacy experts and systems security experts).
- EFT/POS services operate on-line and are widely available to consumers, a financial data trail is created each time the service is used;
- the time and location of each transaction is recorded, allowing the opportunity for private sector parties to effectively conduct surveillance on consumers;
- the use of EFT networks, whereby a customer from one financial institution can use the facilities of another institution, requires shared EFT systems, which could permit access by a number of financial institutions to an individual's financial information, and which could then be without the knowledge or consent of the individual;
- systems exist where certain EFT services are offered in foreign countries, which allows foreign financial institutions access to personal financial information;
- the proliferation of POS systems linked to the use of private cards has the potential to allow private organizations to collect and store large amounts of detailed purchase information. This provides business with the necessary information needed to target markets and more effectively direct advertising campaigns; and
- EFT systems sometimes rely on telecommunications equipment, which presents the possibility for unlawful interception of personal financial information with intercepting devices.

Generally, Canadian financial institutions' obligations regarding the use of consumers' personal data are addressed in four ways. First, the policy rules and by-laws of the Canadian Payments Association address the privacy of personal information in EFT systems. However, these rules and by-laws are not known to consumers. How violations are treated is not transparent to consumers. Second, contracts exist between consumers and financial institutions. In theory, violations are actionable under contract law. However, consumers are entering into contracts of adhesion that place the onus on the individual consumer to prove harm. (Many consumers, for example, do not retain transaction records after using ATMs. This means that financial institutions retain all of the evidence in cases of dispute. The fact that transaction records to not have standing as receipts under the law also places consumers at an evidentiary disadvantage in cases of dispute.) It should be noted that the financial products associated with the relevant contracts, such as bank cards, are issued on a take it or leave it basis. Third, and in addition to contract law, there are common law rules that ... "regulate the use of information that is disclosed to financial institutions on a confidential basis".[26] It should be recognized that this offers only limited protection. Fourth, and to address concerns about privacy, the Canadian Bankers Association (CBA) completed work in 1990 on a model privacy code affecting bank customers for its member

---

[26]"Regulating the Financial Institutions: Protecting the Privacy of Customers' Personal Information". A report submitted by the Privacy Commissioner of Canada to the Standing Senate Committee on Banking, Trade and Commerce. 1992, p.2.

institutions based on the OECD Guidelines. In turn, the CBA members are introducing their own codes based on the model. This initiative is discussed later in this paper. Other federally and provincially-regulated financial institutions have not completed the development of privacy codes.

Horizontal Integration/Financial Conglomeration

In amendments to major statutes governing financial markets, the federal government has made it possible for financial institutions to acquire controlling or lesser interest in other financial service institutions.[27] The potential impact of this new legislation on privacy relates to whether and how institutions share client information with their affiliates and the degree to which consumers are made aware of or can consent to the sharing of information about them. **The principle policy question arising from the horizontal integration of financial institutions is if a consumer enters into a relationship with a bank, does he or she also enter into a *de facto* relationship with the bank's affiliates? If the answer is affirmative, a related question is what are the bank's confidentiality obligations to the consumer vis-à-vis personal information?** There is a spectrum of possible answers to the latter question ranging from a free flow of information to absolutely no flow of information, with various degrees of restriction in between.

The Standing Senate Committee on Banking, Trade and Commerce recently commented on the deposit-taking institutions' relationships with their insurance subsidiaries.[28] While giving consideration to the insurance business (banks) regulations and not directly citing privacy issues, but rather the effects of free flows of information on competitiveness in the insurance industry, the Committee recommended:

> ...that the regulations governing the business of insurance by deposit-taking institutions ensure that a deposit-taking institution not be permitted to pass any information respecting its customers and the employees of its customers to any entity, except for that related to the administrative function with respect to the authorized types of group insurance.[29]

Although specific regulations on privacy are absent from the acts, each, except the Cooperative Credit Associations Act, empowers the Governor in Council to regulate the "use ...of information supplied...by its customers".[30] **A policy question concerns the role of governments in determining whether more stringent privacy standards are required and what those standards might be.**

---

[27]Amendments to the Bank Act, Trust and Loan Companies Act, the Insurance Act and the Cooperative Credit Association Act, proclaimed in force June 1, 1992.

[28]Twelfth Report The Standing Senate Committee on Banking, Trade and Commerce. (May 5, 1992), pp. 3-7.

[29]Ibid., p.7

[30]The Submission by the Privacy Commission to the Senate Committee op. cit., p. 2.

Telecommunications

The need for information in our economy has driven the development of quick and efficient telecommunications technology. This capability raises its own privacy concerns. The new technology creates potential privacy risks associated with, for example, with cellular phones. Another group of services know as "personal identification number services", such as, caller identification (caller I.D.), automatic number identification and personal communications systems, which rely on personal telephone numbers, present pervasive threats to privacy.[31]

The fact that the telecommunications industry depends so largely on technology for innovation raises two new policy questions: first, the need by regulators to guarantee existing levels of privacy for individuals when new technology is introduced (privacy neutrality) and second, the need for consumers to be able to maintain existing levels of privacy, when new technology, is introduced without the imposition of additional costs (cost neutrality).

Cellular Phones

Cellular telephones are a wireless form of communication (radios) whereby signals are beamed back and forth between the cellular phone user, telecommunications satellites, and centralized relay stations. The primary resulting threat to privacy is that these signals are more easily intercepted and monitored by third parties than traditional wired telephone transmissions. Information about the enhanced susceptibility to surveillance was not made widely available by telephone companies at the time the new technology was introduced. As the popularity of these devices increases, so too will the potential for increasing numbers of unwanted invasions of privacy. Technological developments will offer some enhanced resistance to interception but likely at an increased cost. **Key policy questions are: whether penalties, as a deterrent against those who would attempt to intercept signals, may be seen as an important element of security and a key aspect in determining user confidence; and similarly, whether future guidelines that take into consideration security limitations may be required for businesses that wish to use cellular technology to transmit personal data.**

Caller Identification

This service is one in a grouping of services more formally known as a call management service (CMS). This feature enables the person being called to view the telephone number of the person who is calling. Using the service, subscribers can screen unwanted phone calls and discourage abusive and obscene phone calls. Agencies which offer emergency services (police, ambulance, etc.) can trace phone calls where the caller may not be able to communicate verbally.

---

[31]See Rideout *Op cit*, p. 9.

There are, however, also some drawbacks to caller I.D. One example that has received extensive regulatory scrutiny in Canada and other jurisdictions is that women and children who have fled from abusive family situations can be traced and located through caller ID, should they attempt to contact the abusive spouse. A second is that it eliminates the security of unlisted numbers. In debating privacy aspects of caller I.D., critics argue that the technology causes the transfer of personal control from the consumer to the telephone company. In essence, the service requires that the telephone company decides when the phone numbers of individual consumers will be disclosed to a third party in that the phone company sells the number doing the calling to a call recipient who is a subscriber to caller I.D. In some jurisdictions, this has required the caller, who does not want to disclose his/her number to pay for what is known as call blocking, that is, preventing the release of the number.

A major marketplace application of caller ID is the linkage, known as automatic numbering identification (ANI). The use of ANI enables a business to immediately retrieve computer files containing customer information. It does this by automatically linking a caller's number and the customer's name and records which then appears instantly on the operator's screen. Major home pizza delivery services often use this technology as do other neighbourhood retailers. In a larger application, American Express Co. used to require its operators in the United States to greet calling customers by name. The practice of greeting customers by name was discontinued when the company received extensive negative feedback from customers.[32] However, the use of ANI continues and the question remains as to the need for restrictions on the security, accuracy and circulation of information gathered and linked in this manner.

Another CMS introduced with caller ID was call blocking. This feature allows the calling party to have his or her number blocked from subscribers to the caller ID service. The introduction of call blocking has, however, sparked a new debate about whether the phone companies should charge a fee for the service, as they did at its introduction, or offer it free of charge to those wishing to ensure that callers using ID services could not read their telephone numbers. A recent decision by the Canadian Radio-television and Telecommunications Commission (CRTC) states:

> ...that the provision of per-call automated blocking free to those subscribers who so request it...would allow subscribers to maintain the level of privacy they perceive necessary without the burden of incurring a charge to do so.[33]

There was reluctance on the part of some telephone companies to comply with this decision.

---

[32]Peter Coy "Why All the Heavy Breathing over Caller I.D.?" Business Week June 18, 1990., p. 34.

[33]Telecom Decision CRTC 92-7 Call Management Service - Blocking of Calling Number Identification.

Personal Phone Numbers/Personal Communications Systems

Telephone companies in the United States have began issuing permanent telephone numbers to cellular phone users. Since customers will be assigned a permanent phone number for life, it becomes a useful unique identifier. The phone number facilitates the matching and collecting of personal information from various sources. It also allows private enterprise to track individuals. While the service is not yet offered in Canada, its introduction linked to cellular phones is anticipated. The concept of common identifiers is treated separately under a discussion of federal/provincial issues.

Transportation

A major concern in the transportation sector is the use of airline computer reservation systems (CRS) to collect, use and possibly circulate personal information based on data collected at the time a reservation is made. This could include substantial amounts of personal information such as name, age, nationality and even dietary requirements.

Additional detailed travel information can be collected by travel agencies. This information includes preferences in lodging, meals, and seat selections. Ostensibly this data is used for frequent travellers who would rather not make detailed demands for particular services each time they visit their travel agents. The information, however, can undoubtedly be used for other purposes. While some associations of travel agents have developed privacy codes respecting the use of personal information there are no apparent legal restriction on its use by other businesses that cater to travellers (airlines, hotels, restaurants, resorts, etc.). **The policy questions that arise concern the right of airlines and travel agents to disclose this information to third parties without the informed consent of the consumer and whether periodic review of consent should also be required. A third question is the extent to which airlines should be required to disclose to consumers the existence of files containing travel-related personal information and provide consumer access to these files.** The need for inter-jurisdictional cooperation is also a concern. While the regulation of airlines CRS's is likely to be a federal responsibility, regulation of the information collected and retained by travel agents and other industry members such as hotels likely rests in provincial jurisdictions.

Other issues arise when travel takes place outside the consumer's country of residence. Domestic laws may not be applicable in ensuring privacy. Thus, consumer protection from transborder data flows are also a major concern. Recognizing the possible infringements on consumer privacy rights, the International Civil Aviation Organization (ICAO) has adopted a code of conduct regarding CRS information privacy. The code recognizes the airlines' need to collect and disseminate personal information, within and between national borders, to certain sources in order to accommodate customers' needs. The ICAO requires the users of the CRS to recognize the sensitivity of the data and thus take measures to ensure its security. The code refers national governments to the International Air Transport Association Recommended Practice 1774, "Protection of Privacy and Transborder Data Flows of Personal Data Used in International Air Transport of Passengers and Cargo", for guidance. **A policy issue arises from the fact that Canada has not yet adopted this code.** While, in practice, the operators of CRS services have gone to

considerable lengths to limit the circulation of what are called personal name records, Canadian owned and operated airlines do not yet adhere to a recognized standard for the gathering and circulation of this type of data.

Database Marketing

The general privacy issues identified at the beginning of the paper arise most obviously in the relationship between database marketers and consumers. Consequently, one or more of the policy questions raised in other sectors, such as financial services and telecommunications, may also apply to the direct marketing industry.

The development of sophisticated data processing systems enables businesses to manipulate and use personal information to define and target market groups for the company's goods or services. With these types of consumer profiles, the company can direct its solicitation directly to the consumers who would most likely buy from the company. This is generally known as "database marketing". It can include financial information such as credit card numbers and other personal information. It has also been described as the trafficking of information in that it is a commodity with value developed without individual consent.[34]

The personal data that direct marketers need in order to target market effectively can be obtained from various sources. Examples of this include donating to charitable or political organizations, entering sweepstakes, calling or writing a company for information, buying from a catalogue or subscriptions or in some cases, being registered in a provincial motor vehicle or land registry. Using this information, companies can then create lists based on profiles of groups that they wish to target. For example, if a clothing company finds that most of its customers are middle-income, university-educated men between the age of 30 and 35, then a list fitting those criteria can be created from the company's own database, bought from another direct marketer, or it can be a hybrid list composed of information collected and matched from various databases. Other than proprietary considerations, there are generally no restrictions on list building or on list circulation.

Database marketing raises privacy concerns. **A policy question concerns the need for limits on the amount and type of information an organization should be allowed to collect.** Consumers are likely to be wary if they are required to give detailed personal information regarding income, marital status and other intimate information in order to receive a good or service. If excessive amounts of information are demanded, then it is an indication that the organization may have motives other than solely providing goods and services. Thus, **there is also a policy question concerning the need for full disclosure of the reason the data is being collected. This reflects the general marketplace principle requiring marketplace transparency in all transactions and interactions.**

Direct marketers in Canada currently do not need the customer's consent in order to sell a database containing personal information. While consumers can have their names

---

[34]See Rotenberg in Rideout, *Op cit*, p. 4.

removed from mail order lists owned by members of the Canadian Direct Marketing Association (CDMA), non-members need not comply. Name deletion from telemarketing lists is much more problematic even though the CDMA offers this service and it is mandatory for its members. The service is relatively new, it is extremely expensive to operate and cannot guarantee the behaviour of companies that are not members of the CDMA. **The policy question arising here is the degree to which consumers should be able to control how their personal information is used and to whom it is circulated.**

A discussion by the industry of "benefits" arising from direct marketing is affected from the consumer perspective by the telephone. The telephone elicits strong concerns about the invasion of personal privacy and its use in telemarketing creates a stronger negative reaction that direct marketing by mail.[35]

FEDERAL/PROVINCIAL/TERRITORIAL PRIVACY ISSUES

Responsibility for many privacy issues can be assigned to the appropriate level of government on the basis of divisions of powers. There are, however, privacy issues that seem to require the attention of the federal and provincial/territorial levels of governments.[36] Some of the more prevalent issues include the use of Social Insurance Numbers (SIN), medical records, retail and post retail transactions, extended warranties, and out of country data storage.

Social Insurance Numbers/Common Identifiers

Canadians are sometimes asked to supply their Social Insurance Number (SIN) when purchasing goods and services. The SIN was introduced in 1964 as an account number for Canada and Québec pension plans and unemployment insurance contributions. On the basis that "no two SIN's are alike", the use of this type of unique identifier facilitates the collection, matching and manipulation of consumers' personal information. It becomes a file number that can be used to draw information from different sources.

Some conditions exist on the use of a SIN. For example, it is illegal to use a SIN without a person's authorization. If permission is granted to another person or organization to use a SIN, for reasons set forth in the Income Tax Act, the number cannot then be used for any other purpose. If, however, a person or organization requests a consumer's SIN without specifying its intended use, it can be used for any purpose. Further, it is not illegal for a business to refuse to deal with any consumer who does not supply his or her SIN on request as a condition of completing a transaction. The consumer has no recourse in such cases except the power of exit. However, there seems to be little understanding in the private sector that an inappropriate use of the SIN could jeopardize personal privacy.

---

[35]See Report: "Public Concerns Over Privacy: The Phone is the Focus" in Telecommunications Policy, April 1991.

[36]For example, see "Regulating the Financial Institutions: Protecting the Privacy of Customers' Personal Information".

The extent to which the use of the SIN can be taken beyond the scope of its intended use is demonstrated in the example of a current credit card agreement issued by a major financial institution.

> "Credit information: You may give to and obtain from persons with whom I have or may have financial or other business dealings (and commercial and consumer reporting agencies) credit and other financially-related information about me. If I have supplied my social insurance number in any application to you, you may treat my social insurance number as an integral part of that information and maintain it in your records about me. You may likewise use my social insurance number and communicate it and allow it to be communicated to those persons and agencies as an aid to identify me. This Section will continue to apply after the termination of this Agreement for communications and uses of the nature outlined above."

The privacy issue, then, is rooted in the use of the SIN as a unique nationally based file number for business to increase its access of information about individual consumers. **The policy question is whether there should be restrictions on the use of the SIN, as well as other unique identifiers, such as telecommunications applications, drivers licenses and credit card numbers.** The options could include prohibiting the use of any national identifier, limiting the use of the SIN and other identifiers, except in a few specific well-defined situations, and aside from the few well defined exceptions, giving the consumer the opportunity to opt out of providing his or her SIN, or any other identifier, to a business without the threat of the business refusing to deal. With regard to the use of common identifiers, it should be noted that some states in the United States have banned the use of credit card numbers as identifiers but primarily because of credit card fraud considerations (misappropriation of credit card numbers).

The effectiveness of restricting the use of the SIN is in itself dubious. Unless prohibited, restrictions on the use of the SIN are likely to encourage some major businesses to adopt new national identifiers. Furthermore, the cost of developing such identifiers would likely be passed on to consumers.

It is significant to note that the federal government has taken some steps to restrict its use of SIN's within government.[37] The SIN cannot be used for many functions including employee numbers. The federal government has also restricted its use in the private sector as an identifier in record-keeping systems by the federally-regulated insurance industry.

In other jurisdictions, such as Germany, Sweden and the United States, discussions about the development of personal identification numbers has been instrumental in the movement to develop national data protection. Most nations have issued numbers as an aspect of identification and authentication for government based social service programs. However, except in war times no western democratic governments have issued unique

---

[37]On the other hand, there has been a recent case where payment of an infant's medical expenses have been denied under the provincial medicare system (P.E.I.) because the parents refused to obtain a SIN for their child.

numbers which follow the citizen from birth to grave[38] and which could be unilaterally co-opted for use by the private sector.

Medical Records

While the general policy questions stated at the beginning of this paper apply to personal medical information, the specific concerns arise from the disclosure of medical information to third parties by doctors or other medical facilities without the informed consent of the individual. This is an area of potential conflict where personal information in the form of case histories could be made available to the private sector for research or to the insurance industry as a research paper to a professional journal. **A policy question arising from this situation is whether in all cases there should be limits applicable to the circulation of such records.** This also raises the issue of the ownership of medical information.

Changes in technology will continue to keep privacy concerns about health records in the public eye and whether existing controls on health cards (such as Ontario and Québec) are adequate. **The advent of smart cards containing confidential information raises a policy question about the need for the parallel development of new standards for data security.**

Another major concern is whether patients should have access to personal medical information held about them. As previously noted, this problem was recently addressed by the Supreme Court of Canada. A New Brunswick doctor refused to disclose to one of her patients, medical information given to her by other physicians. Justice LaForest wrote in his decision that "the confiding of the information to the physician for medical purposes gives rise to an expectation that the patient's interest in and control of the information will continue". The judgement established a responsibility of confidentiality for the medical profession, as well as establishing disclosure rights for the patients.[39] The fact that the Court has ruled in this area will likely give rise to further testing of consumer rights and lead to delineation/limitations of the right of the professional and private sectors to act unilaterally.

---

[38]Bennett *Op cit*, pp. 49-50.

[39]Elizabeth McInerney v. Margaret MacDonald: Sup. Ct. No. 21899; June 12, 1992, in Privacy Times, July 1, 1992, p. 4.

OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF DATA

In 1984, the Parliament of Canada accepted the OECD Guidelines as the national standard for the protection of personal information. The Guidelines outline a code of fair information practices to govern the way organizations handle personal information about their employees, customers and the public. The Minister of Justice has been responsible for encouraging the private sector to develop voluntary privacy codes that conform to the OECD Guidelines. Following letter-writing campaigns by previous Ministers of Justice and a Minister of External Affairs, a number of major businesses including, for example, Canada's banks, the cablevision industry and the telephone companies have adopted or are developing privacy codes. In addition, the federal government and a number of provincial governments have adopted comprehensive privacy legislation based, in part, on the OECD guidelines to protect the privacy of individual citizens in their dealings with governments.

The Guidelines address certain concerns. These are:

- Limiting the types of data that can be collected (i.e., no indiscriminate collections) as well as the methods used to collect the data.[40] The general wording of the principle provides the flexibility to address the sensitivity of certain data based on its nature, the context of its use, and various other criteria that may be specific to particular cultures.
- Ensuring that the data being collected is relevant for the purposes for which it is being used, as well as ensuring that the data is kept up-to-date, accurate and complete. This is particularly important in situations where faulty data can result in actual harm to the data subject.[41]
- Requiring that data collectors specify all of the purposes the data will serve prior to its collection. Subsequent changes of purpose should also be specified and should remain relevant to its original purpose. It further requires that once the data no longer serves a purpose, it should be destroyed or given an anonymous form.
- Restricting the use of the collected data to only those purposes defined unless the informed consent of the data subject is first obtained.
- Prohibiting the disclosure of information to third parties without the express consent of the consumer unless authorized by law.[42]
- Providing sufficient security safeguards. These could include physical measures, such as locked doors; organizational measures, such as assigning various levels of security clearance to various employee and management levels; and systems measures such as enciphering.

---

[40]Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD (Paris, 1980), p. 29.

[41]Ibid., p. 30

[42]Ibid.

- Providing the individual with the opportunity to access any files containing personal information being held by a second party. This should not require an unreasonable cost of time or money to the consumer.
- Providing the individual with the opportunity to ascertain that another party has information concerning him or her; to have that data communicated in a readable form; and to challenge the data.[43]
- Placing responsibility for adherence to any codes or laws based on the OECD Guidelines on the data controller, even when processing is being conducted by someone else on his behalf.[44]

The Guidelines also deal with their international application. The basic thrust of these paragraphs is that no country should implement laws which unfairly restrict the flow of information between countries and that any flows should be secured.[45]

To date, all OECD members have adopted the OECD Guidelines with varying degrees of compliance. Canada, for example, has implemented comprehensive privacy legislation regulating the collection and use of personal information by the federal government, as have the provincial governments of Ontario, Québec and Saskatchewan. (Legislation in British Columbia comes into force in 1993.) Canada's policy of encouraging voluntary adoption of privacy codes in the private sector, however, has had limited success. Few industries to date have implemented codes although the need for negotiated voluntary codes has become more apparent. The Canadian Standards Association is spearheading an effort by governments, private sector organizations and consumer organizations to develop a national privacy code for use as a model by individual businesses and trade associations. In contrast to Canada, countries such as Germany and Ireland have more comprehensive data protection laws that regulate both the public and private sectors.[46] Although there is considerable debate in North America about actual levels of compliance in Europe where legislative protection exists and what this might mean for privacy protection in Canada, national governments in Europe have developed compliance instruments in accordance with their own cultural and political environments which makes judgements by outsiders on the effectiveness of compliance difficult.[47]

There has been some criticism of the OECD Guidelines. The first is the claim that technological advancements have rendered the guidelines obsolete and possibly ineffective. In response, and to ensure that the Guidelines remain timely and relevant, the OECD has arranged to have them reviewed and, if necessary, revised annually.

---

[43]Ibid.

[44]Ibid, p. 32.

[45]Ibid.

[46]"Privacy and Data Protection: Issues and Challenges" a report prepared for the Ad Hoc Experts Meeting on Data Privacy Protection. OECD. (November 1991), pp. 6-10.

[47]See Bennett *Op cit*, chapters 6 and 7.

Secondly, concern has been raised that current draft guidelines being considered by the OECD on systems security may in some ways be in conflict with the existing privacy guidelines. Aspects of systems security principles could be interpreted to require monitoring the existence of data communications. The concern in the particular situation is that principles of systems security can be interpreted to infer a distinction between secrecy of message content and secrecy of systems usage, a distinction that the OECD Privacy Guidelines do not recognize. Privacy advocates are working to ensure increased security in both areas.[48]

A third concern is the impending adoption by European Community (EC) members of a revised directive on privacy. The directive, if passed in its present form embodies strict requirements on transborder data flows and would curtail transborder flows except to those non-EC countries that possess adequate data protection regulations in accordance with the EC Directive. The current anxiety among some national governments that have adopted the OECD Guidelines is that voluntary compliance may no longer be considered acceptable by the European Community, resulting in the potential imposition of trade restrictions within the EC.

THE EC DIRECTIVE ON PERSONAL DATA PROTECTION

The European Community (EC) is committed to the development and implementation of policies designed to harmonize the political and economic relationships between its current twelve member states. One such policy, which has relevance to consumer privacy,is the EC Directive on the protection of individuals in relation to the processing of personal information.[49] The purpose of the directive is to offer a uniform level of data protection for consumers in order to facilitate the free flow of transborder data.

Canada has several concerns with the directive. Of particular interest is Article 24. This article states that:

> The Member States shall provide in their law that the transfer to a third country, whether temporary or permanent, of personal data, which are undergoing processing or which have been gathered with a view to processing, may take place only if that country ensures an adequate level of protection.[50]

---

[48]James A. Katz, "Social Aspects of Telecommunications Security Policy" Telecommunications Policy, August 1990, pp. 324-332.

[49]"Draft Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data" Com (90) 314 Final - SYN 287 (July 1990). A new draft document has been released but is not yet available.

[50]Ibid, p. 22.

This could represent a potential non-tariff barrier (NTB) to trade. There are also some concerns about this article among privacy experts. The first is the failure of the EC to define "adequate protection". Protection can be interpreted in many ways. Without such a definition, the legislation is rendered effectively meaningless.

The second concern is closely related to the previous one. Clear and precise definitions of criteria for measuring enforcement/sanctioning capacity would be required in order to maintain some form of objective evaluation.

A third concern is that different cultures have different values and perspectives on privacy which may be irreconcilable with the EC's concept of "adequate protection". Thus, privacy criteria adopted by national governments may represent a non-tariff trade barrier based on culture rather than on merit.

In addition to applying the same general principles as the OECD Guidelines, the EC Directive also establishes mechanisms to oversee the implementation and adherence to the directive's stipulations. The directive is also more specific than the OECD Guidelines in defining the rights and obligations of the data controller, the data subject, and the Member States.

Thus a policy question that arises from the efforts of the EC to adopt a privacy directive is whether there is a need to determine the meaning of "adequate protection", given cultural differences.

CANADIAN ACTIVITY

The growing privacy concerns of the public and government have driven some activity to address the issue at the federal, provincial, and sectoral/industry levels. These initiatives range in substance from comprehensive to superficial.

Federal

For analytical purposes, federal activity on the privacy issue can be broken down into three types: legislative, non-legislative policy, and Supreme Court rulings and Charter of Rights and Freedoms interpretation.

Legislation

Federal legislation dealing specifically with personal privacy is limited to regulating public sector institutions, although there are statutes that impinge on privacy or have provisions to incorporate privacy regulations into the statutes, should the need arise. The Privacy Act (1982), which was based on the OECD Guidelines, was the federal government's response to the public's concern about potential for the abuse and misuse of personal information by government. The Privacy Act limits the federal government's ability to collect, use and disclose personal information without the individual's informed consent.

Other legislation with privacy implications include the Criminal Code, which deals with restrictions to wire tapping and other interceptions of personal communications; the Statistics Act and other legislation, which prohibits the disclosure of personal statistical and other personal information; and the Income Tax Act, which sets limitations on the use and disclosure of personal income tax information.

Several pieces of legislation currently do not have privacy regulations embodied in them, however they do have provisions which would allow for the incorporation of such stipulations. Some examples include the Bank Act (Section 459), the Trust and Loan Companies Act (Section 444), the Insurance Act (Section 489) and the Telecommunications Bill (Section 7 and Section 46) now before Parliament. Thus, should the need arise, the government would have legislative authority in certain sectors.

Non-Legislative Activity

A recent initiative launched by the federal Department of Communications (DOC) is an example of the government's current policy of encouraging the private sector to develop voluntary codes based on privacy principles. On June 29, 1992, the DOC released a discussion paper and proposed privacy principles for the telecommunications sector.[51] These principles require:

---

[51] Privacy Protection in Telecommunications: Discussion Paper and Proposed Principles. Department of Communications. June 1992.

- the explicit recognition of privacy considerations in the provision, use and regulation of telecommunications services;
- informing the public of the implications that telecommunications services rests with the service providers and government;
- actions at no cost to the consumer, to maintain static levels of privacy whenever new technology affects privacy;
- that there should be limitations to the collection, use, and disclosure of information generated by telecommunications services, and only with the informed consent of the consumer, and;
- there should be methods of protecting telecommunications information, including a periodic review, in order that changes can be made to correspond to the public's changing expectations about privacy.

The principles have been the basis for a public consultation process, through which amendments will be made before they are released in their final form. The Minister of Communications, the Honourable Perrin Beatty, has announced two possible methods of applying these principles. The first, which the Minister has publicly stated is his preference, is to encourage the voluntary adoption of the principles. The second possibility, which could arise from the public consultation process or from industry inaction, is that the principles could become licensing requirements administered by the CRTC under the Telecommunications Act, now before Parliament.

Supreme Court Decisions and Charter Interpretations

The third type of activity at the federal level is Supreme Court judgements. The Supreme Court, which is the final court of appeal in Canada, provides jurisprudential privacy protection in several areas. Most rulings, however, have not dealt with informational privacy, but rather criminal cases relating to search and seizure and the use of electronic surveillance.[52] There has also been one case relating to a refusal to fill out a portion of the census for personal reasons. The Supreme Court ruled that filling out the census is sometimes an invasion of privacy.

---

[52]Mario Duarte v. Her Majesty the Queen, and Santiago v. The Queen, for example. The court's ruling in both these cases were based on Section 8 of the Charter of Rights and Freedoms, which guarantees protection from unreasonable search and seizure.

PROVINCIAL

Currently, the bulk of statutory privacy protection in the provinces is limited to information collected and used by the government. Provincial governments that have access to information laws include Manitoba, New Brunswick, Newfoundland, Nova Scotia, Ontario, British Columbia, and Quebec. These offer the same basic provisions as the federal Access to Information Act, where citizens are allowed access to government documents except in certain specified cases. However, of these, only Québec, Ontario, Saskatchewan and British Columbia[53] provide comprehensive legislative protection with respect to the collection, processing and disclosure of personal data by the respective government.

The Québec government could be the first to introduce legislation affecting the collection, use and disclosure of personal data in the private sector. The Québec government has drafted a bill which may be based, in part, on the OECD Guidelines and the EC Directive. It should be noted that Québec already has some guarantees of data protection as contained in the 1991 amendments to the Civil Code as well as in the Québec Charter of Rights and Freedoms.

As mentioned in the introduction to this paper, invasion of intellectual privacy has no specific tort of its own, but can be actionable under the torts of trespass, nuisance, defamation and breach of confidence. Common law protection, however, is sparse, and has considerable limitations. The tort most accommodating, that is to say not very accommodating, to the protection of informational privacy is the tort of breach of confidence. Proving this relies on establishing that information was imparted to a party in confidence, and that the information was subsequently used for unauthorized purposes.[54]

Some important provincial court decisions include Canavest House Ltd. v. Lett, where an Ontario Court refused an injunction which would have prevented a computer programmer to use customer lists held by the company for which he was working. The reasoning was that where information is drawn from general trade sources, it cannot be protected.[55] This aided in establishing restrictions for common law protection of personal information. A decision by the Quebec Superior Court in Robbins v. Canadian Broadcasting Corp. (CBC) (1957), found that the CBC had been at fault when the name and address of a viewer of a particular television program was announced on the air with an invitation to write him, after he had written to the CBC to criticize the program. The individual was awarded compensation for damages.

---

[53]B.C.'s Freedom of Information and Protection of Privacy Act was recently proclaimed as law and will come into effect in October 1993.

[54]Coco v. A.N. Clark Ltd. (1969) R.P.C. 41 at 47. In Privacy and the Canadian Consumer, a discussion paper prepared for the Federal/Provincial/Territorial meeting of Ministers of Consumer and Corporate Affairs. Sept 10 & 11, 1990. pp. 2-3.

[55]Ibid.

INDUSTRY RESPONSE

Private sector response to the current government policy on privacy has been slow.[56] Nonetheless, some industries have began to develop their own privacy codes. Some of these privacy initiatives include: the Canadian Bankers Association (CBA) model privacy code for customers; the Canadian Direct Marketing Association draft privacy principles; the Stentor Telecom draft privacy code; and the Canadian Life and Health Insurance Association. These organizations have already drafted codes. There are also other significant initiatives, which are in their infancy and have yet to produce a final or near-final document. One of these is a model code to be produced by the Canadian Standards Association in partnership with government departments, industry associations, private sector companies and other interested stakeholders.

An analysis of some of the codes in industries, where privacy is or has the potential to become a significant issue, will provide a representative portrait of the private sector's response to current federal government policy. The sectors, where there seems to be relatively high levels of concern, are in the banking industry, the direct marketing industry, and the telecommunications industry. As a result of public sensitivity to privacy in these areas, industry associations have either completed or are in the process of developing model privacy codes. The Canadian Bankers Association (CBA) has completed a model code, which its membership is expected to use as a basis for their own codes. (The CBA is now developing a complementary privacy code applicable to bank employees.) The Canadian Direct Marketing Association (CDMA) has drafted a set of privacy principles, which they hopes to develop over the summer of 1992 into an effective part of their code of ethics.[57] Finally, Stentor Telecom Policy Inc. is in the process of developing a "Code of Fair Information Practices" for telephone companies that are members of the Stentor alliance.

CBA Model Privacy Code

While the CBA code offers reasonably close compliance with the eight basic principles in the OECD Guidelines, there is some divergence.[58] One potential privacy problem arises in the code's definition of personal information as any fact that identifies or relates to a specific individual. This excludes the use of opinions and evaluations of customers by banks. This represents an incomplete level of protection since use and disclosure of the opinions and evaluations about an individual, based on factual data and elements of opinion, are as potentially invasive and damaging as the collection, use and disclosure of factual information. The banks take the position that the protection of its credit granting process may require the use of opinions and evaluations although they have recently amended in-house procedures to minimize the amount of information that is collected.

---

[56]See Privacy Commissioner *Op cit*, p. 7-8.

[57]Various government departments have provided feedback on the Association's draft principles.

[58]Privacy Commissioner *Op cit*, p. 7-8

A very general interpretation of the code's data use limitation principle also provides an opportunity for banks to circumvent the intent of the provision. Under this part of the code, there are two areas that require greater specificity. The code requires the customer's consent before disclosing personal information to third parties **except** in instances necessary to protect the banks' interests or out of public duty. New procedures require the signature of a customer acknowledging these conditions. However, the signature consent of a consumer on the form, that is the basis for collecting and storing information, absolves the institution of responsibility for its accuracy and completeness. Both of the exceptions are very flexible and can encompass a wide range of situations that may represent an unreasonable invasion of an individual's privacy. A better definition of "public interest" and setting specific limitations on each bank's interests would strengthen this part of the code.

CDMA Draft Privacy Principles

The CDMA Draft Principles for an Industry Privacy Code, when compared with the OECD Guidelines, are incomplete in several ways. The first is that the wording throughout the document is sufficiently vague that many of the principles could be virtually ineffective. For example, one principle states that direct marketers must give the consumer a "meaningful opportunity...as soon as possible" to opt out of having his or her name used for marketing purposes. Both "meaningful opportunity" and "as soon as possible" are subject to various interpretations, which could provide a sufficient loophole for avoiding compliance.

The draft principles also lack some important provisions. There are no limitations on the types of information direct marketers can collect. Also, while the principles allow the consumer to demand the source of a direct marketer's information about the individual, they do not allow the consumer access to files containing personal information. Nor is there a data quality principle requiring that data be accurate, complete and up-to-date.

While there are deficiencies in the CDMA principles, they do provide a basis for further work. The CDMA has encouraged comments from its members and government and has expressed a commitment to producing a substantive set of privacy principles which will be incorporated into the Association's Code of Conduct.

Stentor Telecom Policy Inc.'s Code of Fair Information Practices

The code covers both customer and employee privacy concerns, and both electronic and paper records. The basic elements of informed consent and customer participation are present in the code. The code further protects personal information disclosed to third parties through contractual arrangements stipulating confidentiality and use limitation conditions. The code also clearly delineates accountability and calls for the establishment of an information ombudsman to handle disputes and complaints. However, the code contains no principle regarding transborder data flows and it defines the information that member companies may collect and keep so broadly that there is little understanding of what, if any, limits might apply.

SUMMARY AND ANALYSIS OF POLICY QUESTIONS

The following is a summary of policy questions and operational considerations arising from a review of sectoral privacy issues.

The summary is intended to highlight the pervasiveness of decisions being made about individuals arising from personal information gathering, manipulation, storage and circulation. It recognizes the experiences of information protection in other jurisdictions and the complexities in addressing some of the policy questions. It suggests that there is reason for Consumer Affairs Departments to further explore specific policy questions. By way of context, it is felt by officials in a number of federal departments that governments would have difficulty responding to a major public outcry caused by perceived unfair business practices linked to the indiscriminate disclosure of personal information to third parties.

The policy questions raised in this paper are of two types, generic, i.e. applicable across all sectors, and those that are sector-specific. The sector-specific questions are usually iterations of the generic questions but with special importance in a given sector. This section will summarize the broad policy questions raised in the paper and identify possible actions that federal and provincial governments can take to address them.

The federal government's current policy is to encourage voluntary adoption of privacy codes by the private sector. This does not exclude the possibility of regulation, should such an approach be necessary.

Generic policy questions

- Is there a need to develop a precise definition for what is meant by "privacy of personal information"?

The need for an understanding is obvious. Governments and the private sector need to know what it is that they are protecting. However, the matter of precisely defining privacy of personal information has not been successful in other jurisdictions where the broader concept of "data protection" is employed and where the passage of legislation has been based on principles of fair information practices, such as the OECD, rather than strict definition arising from responses to specific privacy issues.

- To what extent should there be limitations on the amounts and types of data collected by the private sector and private individuals?

Data should be collected only as a means of providing consumers with goods and services and maintaining a relationship with consumers. Of course, the nature and amount of data needed for these purposes varies from business to business and industry to industry. Thus, a blanket approach to answering this question would not be effective. Rather, it should be approached on a sectoral basis, preferably, on the basis of Canadian principles adapted from the OECD Guidelines.

- What standards, if any, should there be on the accuracy and security of personal data collected by business?
- Should consumers be entitled to access to files containing information about them?

The issue connected with this is that inaccurate personal information can be harmful to consumers. Government regulation in this matter would probably be more justifiable than in any of the other generic issues. This is because, privacy aside, there can be an actual economic loss to the consumer. The problem could be addressed effectively in two ways. The first is by developing data-quality standards for regulatory bodies in various sectors to enforce. The second is by allowing consumers access to any files containing information about them to verify its accuracy and currency.

- To what extent should consumers be given the opportunity to give consent for the circulation of personal information?

Privacy surveys (Harris-Equifax 1991) indicate that the single largest concern among consumers is the loss of control over the collection and circulation of personal data. Requiring informed consent from individuals before collecting and circulating data is one potent way to give control back to the individual consumer.

SECTOR SPECIFIC POLICY QUESTIONS

A number of policy questions arise relevant to the issues in each of the sectors below. Even though the same issues may arise in a number of sectors, responses to the questions will be affected by the impact of different technologies and will necessarily vary.

The likely interest of the provinces and the federal government is recognized in brackets after each of the policy questions.

Financial Services

- In that financial institutions tend to establish, in contract, their right to circulate personal information to whomever they deem acceptable, are new general limits required for the gathering, holding and possible circulation of personal information to third parties by financial institutions? (Federal/Provincial)

- When consumers enter into a relationship with a financial institution, they also unknowingly enter into a *de facto* relationship with its affiliates in that there are few existing restrictions on the circulation of personal information within the corporate entity. Would consumers be better served by the establishment of new confidentiality obligations vis-à-vis the circulation of personal information? (Federal/Provincial)

- What is an appropriate role for governments in determining whether more stringent privacy protection standards are required for financial institutions? (Federal/Provincial)

Telecommunications

- When consumers enter into a relationship with national and transnational conglomerates, they also unknowingly enter into a *de facto* relationship with its affiliates. In this new environment, what are appropriate confidentiality obligations to protect consumers vis-à-vis personal information?

- With the advent of smart cards, such as telephone credit calling cards containing confidential information, there is a perceived need for the parallel development of new standards for data security. What is an appropriate role, if any, for Consumer Affairs Departments in this area? (Federal/Provincial)

- Are more stringent sanctions necessary, as a deterrent against those who would attempt to intercept telecommunications signals, particularly cellular signals? Should Consumer Affairs Departments promote the concept of new sanctions against interception as a key element in determining user confidence? (Federal/Provincial)

- Are standards to protect personal information required for businesses that wish to use cellular technology to transmit personal data, taking into consideration the security limitations of the technology? What is an appropriate role for Consumer Affairs Departments? Other departments? (Federal/Provincial)

Transportation

- Should airlines and travel agents be permitted to disclose personal information such as hotel, restaurant, ticket purchases, frequency of travel and credit information to third parties without the informed consent of the consumer? Where consent is required, should a periodic review of consumer consent also be required? (Federal/Provincial)

- Should airlines be required to disclose to consumers the existence of files containing personal information and should they be required to provide access to these files? (Federal)

Direct Marketing and Other Forms of Retailing

- Is there a need to limit the amount and type of personal information an organization should be allowed to collect - e.g. collection by means of contests, sales contracts, warranty agreements, extended warranty contracts, as well as the type and cost of goods or services purchased and related credit/personal financial information? Is there a need to regulate such limits or should other measures be adopted? (Provincial)

- Should consumers have full access to the personal information held in the databanks of direct marketers and other retailers?

- Should consumers be able to require changes to ensure the accuracy, currency, and completeness of personal information held by direct marketers and other retailers? Should consumers have to pay a fee to access this information?

Social Insurance Numbers/Common Identifiers

- Should new limits be established for the use of the SIN, as well as other unique identifiers, such as permanent telephone numbers, drivers licenses and credit card numbers by non-government organizations? What new general limits are appropriate and what is the role of Consumer Affairs Departments in the process? (Federal/Provincial)

Medical Records

- Should there be new limits on the circulation of medical information by health care professionals to each other, or to third parties in the health care field? (Provincial)

- Is there a need for the development of new standards for data security in parallel with the development of smart cards containing confidential health related information? (Federal/Provincial)

General

- Is there a need for governments/Consumer Affairs Departments to establish the right to existing levels of individual privacy when new technologies are introduced - privacy neutrality? (Federal/Provincial)

- Should consumers be able to maintain existing levels of individual privacy when new technologies are introduced without the imposition of additional costs by service providers - cost neutrality? (Federal/Provincial)

OPERATIONAL IMPLICATIONS

There is a potential for government, both federal and provincial, to come under substantial pressure to provide guarantees against privacy invasions. Consumer interest is unpredictable as is the behaviour of private sector with respect to personal information. Thus, it seems important for governments to keep abreast of developing privacy issues and to create a mechanism to facilitate policy that anticipates or minimally responds to changes in attitudes and technology. One or more of the following options may be an appropriate basis for further work by the federal and/or provincial governments. The options recognize that the privacy of personal information is complex and that initiatives could involve the provinces and the federal government, as well as a number of government departments at each level.

Option #1: The formation of an informal intergovernmental working group of officials at both the provincial and federal levels which would regularly exchange information by teleconference on emerging issues and initiatives in various sectors of the economy. This would provide a uniform level of awareness for Consumer Affairs Departments, as well as an effective mechanism for quickly developing and implementing policy. An informal working group already exists at the federal level and has functioned effectively.

Option #2: Based on the above, privacy should continue to be an agenda item at federal/provincial/territorial meetings of Deputy Ministers of Consumer Affairs to identify areas of mutual concern, share information and coordinate policy.

While there is some disparate evidence to support the claim that the public is becoming increasingly concerned about privacy issues, it has been unclear what level of concern exists and whether it is based on any meaningful knowledge of or experience with privacy issues, including the tradeoff between privacy and marketplace participation. The national privacy survey should provide clear indications of consumer awareness and attitudes. The survey is also likely to indicate a need for consumer information and education about privacy issues.

Option #3: That federal and provincial Consumer Affairs Departments, in conjunction with the private sector, look for innovative means to inform and educate the public about privacy issues subsequent to the national privacy survey. Education would provide the public with a foundation from which to determine what they feel are appropriate actions for both governments and the private sector.

The current federal government policy of encouraging the private sector to voluntarily adopt privacy codes based on the OECD Privacy Guidelines has received slow and erratic response. With growing public concern about privacy invasion, there is a some impetus for action.

It is important, however, that any action taken by the governments target, specifically, those areas of the marketplace where there are problems or the potential for problems since the types of technology and levels of concern in various sectors are different. The blanket approach of extending existing federal or provincial privacy legislation to the private sector would be incompatible with this reality.

Option #4: That the federal and provincial Consumer Affairs Departments more actively encourage voluntary adoption of privacy guidelines through organizations such as the Canadian Standards Association on a sector-by-sector basis. This could be done through letter writing campaigns by Ministers.

Option #5: That the government continue to monitor private sector action on privacy protection, and if it is deemed inadequate, to review the need for other initiatives on a sector-by-sector basis.

Information technology is in a constant state of flux, while codes protecting privacy are relatively static. Similarly, the public's changing expectations about privacy could affect the perceived effectiveness of voluntary codes.

Option #6: Consumer Affairs Departments, in cooperation with industry, could periodically review privacy principle and guidelines to ensure that they take account of technological change and the public's changing privacy expectations. The role of government would be to give advice and suggestions only, in keeping with its preferred policy of voluntarism.

CONCLUSION

Consumer concerns about many of the issues involving the privacy of personal information are latent. There is some evidence, to be tested in a national privacy survey to be conducted this autumn, that Canadians feel strongly that protection ought to exist, in law, with respect to personal information in the private sector, as well as the public sector. For policy-makers, this implies a need to isolate the key issues among the many identified in this summary, to analyze the impacts of privacy protection and to search out policy options which are the least obstructive to individual consumers and commercial interests.