# Information Privacy in Canada (Legislation in the Face of Changing Technologies)

Václav Matyáš, Jr.*†
(matyas@scs.carleton.ca)

**Abstract**

This report provides an overview of Canadian legislation, regulations and policies concerning Information Privacy. Aspects raised by upcoming technological changes and regulations concerning these are examined. The issues related to government agencies, as well as the private sector are given special emphasis. Some of the 'Information Superhighway' issues and considerations in the global North American context are also discussed.

**1991 AMS Classification:** 94-02

**Key Words and Phrases:** Information Privacy, Privacy Legislation, Communication Legislation, Computer Security Policy, Information Superhighway.

*Information and Systems Science program, Carleton University, School of Computer Science, Ottawa, ON, Canada K1S 5B6

†Faculty of Information Science, Masaryk University, Buresova 20, 659 59 Brno, Czech Republic

*"As new technology has brought us the information age, it has underscored the fact that knowledge is often synonymous with power. Information itself has become a commodity - bought and sold in the marketplace and available at our fingertips through computer systems.*

*The information age has made personal information about each of us far more accessible. ... The ease with which information can be collected and disseminated has raised legitimate concerns about the best ways to protect the confidentiality of certain information."*

**George Bush; June 22, 1990, to the "Privacy in the 1990s" conference**

# Contents

# 1 Introduction

In their article for the Harvard Law Review in 1890, Samuel D. Warren and Louis D. Brandeis describe privacy as "**the right to be let alone**". Their article means the beginning of legal thinking on the concept of privacy.

One of the definitions (by A.F. Westin) describes **privacy** as a universal human value with several dimensions:

- **solitude** : the right not to be disturbed,
- **anonymity** : the right not to be known,
- **intimacy** : the right not to be monitored,
- **reserve** : the right to control one's personal information.

In the narrower context of information technologies, privacy can be viewed from two aspects :

- the ability to *control information about oneself and one's activities* ( reserve and anonymity ); and
- the ability to *be protected against unwanted intrusion* ( solitude and intimacy ).

It was observed ([14]) that while privacy experts focus on the privacy implications of telecommunications and computer technology, by contrast the public's concerns with privacy seem to focus mainly on the concrete and visible manifestations of privacy invasion. These appear to be associated with telephone and associated issues.

According to a 1992 poll done by Ekos Research Associates Inc. for the Canadian government and a group of private businesses, **92** percent of Canadians are *concerned* about privacy - **52** percent are '*extremely concerned*'. [2]

The purpose of this report is to provide the reader with a framework representing various jurisdictions, regulations and policies concerning information privacy in Canada.

Section 2 of this report provides a comprehensive overview of Canadian legislation concerning Information Privacy, particularly the federal, Ontario, and Quebec legislation. Different aspects raised by upcoming technological changes and regulations concerning these are examined, as well as issues related to the private sector.

Two model technology applications influencing individuals' privacy - Computer Matching and Call Management Services, and policies concerning these - are described in Section 3.

Some of the 'Information Superhighway' issues and considerations in the North American context are outlined in Section 4. A Summary concludes the report.

# 2 Throughout the Country

Canada's **Charter of Rights and Freedoms** does not provide any explicit protection for privacy. However, judicial interpretations of Section 8 of the Charter, "*the right to be secure against unreasonable search or seizure*", have recognized the individual's reasonable expectations of privacy.

Sections 183 to 196 of the **Criminal Code** also deal with interception of private communications, and state as an indictable offense, punishable by imprisonment up to five years, to unlawfully intercept private communications. A private communication is defined as any oral communication or telecommunication made under circumstances in which *the originator reasonably expects that it will not be intercepted* by any person other that the person to whom it was directed. [15]

Exemptions include, among others, interception with consent of one communicating party or with authorization for *maintaining the quality control or managing of the communication device.*

**Telecommunications legislation** includes a specific reference to privacy protection as a policy objective of the Bill. *This reference requires the CRTC* (Canadian Radio-Television and Telecommunications Committee) *to address privacy issues when exercising its regulatory responsibilities.*

Under the **Radiocommunication Act**, it is recognized as an offense to intercept and divulge any radiocommunication other than broadcasting, e.g. a conversation on a cellular phone, except as permitted by the originator or otherwise permitted under other Act's regulations. It is worth to note here the B.C. Attorney's General incident(interception and later publication of a private conversation over a cellular phone), which accelerated change of the Act in this manner. It is also important to note that, in the area of radiocommunications, interception itself is not an offense unless the communication is used or divulged.

At the provincial level, only Ontario, Quebec, British Columbia and Saskatchewan have legislation concerning explicitly, at least in one part (of their Privacy Acts), data protection. However, these legislations (except in Quebec) restrict access to personal information held by provincial or municipal institutions.

The remaining provinces and territories in Canada do not have legislation concerning *this aspect of privacy.* However, their legislation sometimes provides some protection of personally identifiable data (by restricting access in limited circumstances in the access to information acts, etc.).

The federal Privacy Act restricts access to personal information held by federal government institutions, and provides some conditions for operations on this data, its control, etc. An interesting point is that only Canadian citizens and permanent residents have a right to access their personally identifiable data held by the government institutions.

## 2.1 The Privacy Act - Canada

The federal **Privacy Act** ([5]) came into force in 1983, and was last updated in 1991. The act provides the basic background for protection of individuals' privacy in the manner of information held by the government institutions. The *structure* of the act with section numbers is as follows:

- INTERPRETATION (3)
- COLLECTION, RETENTION AND DISPOSAL OF PERSONAL INFORMATION (4-6)
- PROTECTION OF PERSONAL INFORMATION (7-9)
- PERSONAL INFORMATION BANKS (10)

- PERSONAL INFORMATION INDEX (11)
- ACCESS TO PERSONAL INFORMATION (12-17)
- EXEMPTIONS (18-28)
- COMPLAINTS (29-30)
- INVESTIGATIONS (31-35)
- Reviews and reports ... (36-52)
- OFFICE OF THE PRIVACY COMMISSIONER (53-67)
- OFFENSES (68)
- GENERAL (69-77)

The schedule of ministries and agencies the act applies to includes about **160** institutions. The undisputable fact is that the act might be useful as a basis for the control of information held by government, where consent between the legislative requirements and bureaucratic practice is easier to reach than in non-government sectors, but the challenge of new technologies will surely :

- require changes to the act itself,
- result in the requirement of information privacy legislation applicable to non-governmental institutions as well.

## 2.2 Office of the Privacy Commissioner - Canada

The *Privacy Commissioner* can be viewed as a special ombudsman appointed by and accountable to Parliament, whose office monitors the federal government's operations over personal information. As defined in the annual report ([1]), the Privacy Commissioner's mission is:

- to be an effective ombudsman's office, providing thorough and timely complaint investigations to ensure Canadians enjoy the rights set out in the Privacy Act;
- to be an effective privacy guardian on Parliament's behalf, performing professional assessments of the quality of the government's adherence to the Privacy Act;
- to be Parliament's window on privacy issues, arming it with the facts needed to make informed judgments through research and communications;
- to be the primary national resource centre for research, education and information on privacy.

### 2.2.1 A Privacy Checklist

In order to initiate creation of an inter-departmental working group on privacy and technology and to ensure the governmental actions and service to be up-to-date, the Commissioner has proposed a 'privacy checklist', intended "*to guide senior government officials during the design stage*". The list contains the following points :

- **Openness/Transparency** : Individuals must be thoroughly informed of their rights under the new technologies; given specific notice of their right to refuse to participate(in the use of new technologies), and to be aware of the situations likely to develop around the use of the technology.
- **Informed Consent** : Individuals must be informed clearly and their consent obtained for all uses and disclosures of the information being processed. They should also be able to withdraw consent without penalty.
- **Gate Keeping** : Security mechanisms must be in place to prevent misuse or inadvertent access to individual's data.
- **Matching** : Possible merging or cross-over of personal information during any transaction must be prevented.
- **Access** : Individuals must be given the right of access to and correction of information regarding themselves.
- **Non-Discrimination** : New technologies must not limit the government services.
- **Beneficence** : Government must acknowledge and affirm that new technologies are tools to help deliver service to individuals and **not** instruments to enable it to exert control over individuals' information.
- **Respect** : All intermediaries must respect principles of privacy ethics and laws.
- **Responsibility** : Those entering information into systems must exercise the highest standard of responsibility to ensure the reliability of the system.

### 2.2.2 Other Activities

One of the past Commissioner's activities - alert to the threat to privacy by *interception of cellular telephone calls* - urged Parliament to protect the privacy of cellular phone users. The government, through Bill C-109 introduced amendments to the *Criminal Code* and the *Radiocommunications Act* to make it illegal to intercept private cellular phone conversations maliciously or for gain; and the Criminal Code amendments also expand the definition of a *private communication to include* **encrypted** *radio based communications.*

The Office also had begun work on broad telecommunication principles, and influenced the Canadian Radio-Television and Telecommunication Committee (CRTC) "*caller I.D. decision*", which, being a reversal of an earlier verdict, put to rest perhaps the most controversial issue arising from the introduction of Call Management Services by telephone companies. In the end, the CRTC required all companies in its jurisdiction to provide free per-call blocking for callers who did not want their numbers displayed. (viz. section 3.2)

Other influence and cooperation issues of the Office's involvement into the privacy awareness resulted in creation of other private sector privacy codes, which are also briefly mentioned in other parts of this report. However, it would appear that *nation-wide legislation for the private sector rather than voluntarily accepted codes*, would be of more use.

Inquiries to the Office increased by 10 per cent from 1992 to 1993 - to 5,183 ; 20 per cent of these were concerning privacy matters over which the Privacy Commissioner has no jurisdiction, namely other public sector organizations or private businesses. An interesting fact is that

Figure 1: Personal Information and the Federal Government

more than 10 per cent of the inquiries were about the SIN, mostly about individuals' concern about providing their SINs to organizations and other individuals (landlords, etc.) not subject to any legislation covering the SIN.

A key group of departments which hold information on most Canadians consists of **Revenue Canada, Taxation**, **Health and Welfare Canada**, **Employment and Immigration** and **Statistics Canada**.

## 2.3 Ontario - Freedom of Information and Privacy Act

The *Freedom of Information and Protection of Privacy Act* (the provincial *Act*) and *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act*) are both within Ontario's jurisdiction. Because of their similarity, this part of the report will briefly describe only the provincial Act, and then discuss some interesting implications. The provincial Act implies, like almost all North American legislation, only to governmental agencies, in the number of **239** at this time.

### 2.3.1 The provincial Act

The Act ([21]), introduced in 1987, and with the last Amendment from 1992, consists of five parts, with the following structure (numbers of sections are added for further references) :

- PART I - ADMINISTRATION (3-9)
- PART II - FREEDOM OF INFORMATION
  - ACCESS TO RECORDS (10-11)
  - EXEMPTIONS (12-23)
  - ACCESS PROCEDURE (24-30)
  - INFORMATION TO BE PUBLISHED OR AVAILABLE (31-36)

- PART III - PROTECTION OF INDIVIDUAL PRIVACY
  - COLLECTION AND RETENTION OF PERSONAL INFORMATION (37-40)
  - USE AND DISCLOSURE OF PERSONAL INFORMATION (41-43)
  - PERSONAL INFORMATION BANKS (44-46)
  - RIGHT OF INDIVIDUAL TO WHOM PERSONAL INFORMATION RELATES TO ACCESS AND CORRECTION (47-49)
- PART IV - APPEAL (50-56)
- PART V - GENERAL (57-70)

Among other useful information and statements provided by the act, let us note the definition([21]) of *record* for the Act's purposes :
**"record"** means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes :

- correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof; and
- subject to the regulations, any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.

### 2.3.2 Providing Notice of Collection

Section 39(2) of the provincial Act states that when collecting personal information, unless an exception applies, an institution **must** provide ([11]) the individual to whom the personal information relates with notice which includes specific details on the following three requirements :

1. the legal authority for the collection;
2. the principle purpose(s) for which the personal information is intended to be used; and
3. the title, business address and telephone number of a person employed by the institution who can answer questions about the collection.

Notice may be provided either orally (in person, over the phone); or in writing (on an application form, posted sign, etc.).

However, sections 39(2) and (3) of the provincial Act state that the notice requirement does not apply where :

- the Minister waives notice;* or
- *a law enforcement exemption is cited.*

*this option would seem to require a further explanation

### 2.3.3 Copying Information to Individuals Inside and Outside an Institution

**Within the Institution**(government department, agency, etc.) a record should be copied only for staff members who need it in the performance of their duties; the record should not be copied for an individual for information only (unless one of the specific circumstances enumerated in sections 32 or 42 applies).

A *"c.c."* listing should appear on the original correspondence, indicating all parties who are receiving copies.

**Outside the Institution** - before a decision is made to copy a record containing personal information to a party outside of the institution, it should be considered whether the individual to whom the information relates might reasonably expect such a disclosure. [8]

### 2.3.4 Responding to Requests for Personal Information

**Records that contain any of the requester's personal information**

*Generally, an individual seeking access to a record that contains his/her personal information has a greater right of access than if the record does not contain any such information.* Part III of the provincial Act obliges institutions **to consider** whether records should be released to an individual, regardless of the fact that they may otherwise qualify for exemption under the legislation. In these situations, the institution has the discretion to choose whether to release the records after considering any applicable exemptions and weighing the requester's right of access against any other individual's right to the protection of his/her privacy. [12]

**Records that contain personal information of an individual other than the requester**

Such requests are to be evaluated under Part II of the provincial Act. Where the record contains only the personal information of an individual other than the requester, the institution must refuse to disclose this information, except where its disclosure would **not** constitute an unjustified invasion of the individual's personal privacy, or where another exception in section 21(1) of the provincial Act applies. [12]

### 2.3.5 Third Party Information at the Request Stage

Dealing with requesters seeking access to third party information, the government organizations are required to give written notice of the request to persons to whom the information relates (*third parties*) and to *seek their views on whether or not the information should be disclosed.* These cases apply to situations like neighbour complaints, accident witnesses' statements, government contract competitions, etc. [9]

## 2.4 Ontario - Office of the Privacy Commissioner

The *Information and Privacy Commissioner* (IPC) acts under both sections of the Ontario privacy legislation - *Freedom of Information and Protection of Privacy Act* (the provincial *Act*) and *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act*).

The **mandate** of the IPC is executed in five ways :

1. resolving appeals when government organizations refuse to provide requested information;

2. investigating privacy complaints about government-held information;

3. ensuring that government organizations comply with the Acts;

4. conducting research on access and privacy issues and providing advice on proposed government legislation and programs; and

5. educating the public about Ontario's access and privacy laws.

The Information and Privacy Commissioner reports to the Legislative Assembly of Ontario. The present Commissioner(Bruce Phillips) was appointed in 1991 for a five-year term.

Each year, provincial and municipal government organizations report to the IPC on their activities under the Acts. In 1992 provincial ministries and agencies received 9066 requests under the provincial Act (37 per cent above the annual average over the previous four years); municipal government organizations received 7139 requests in 1992.

### 2.4.1 Other Activities

Whether or not certain records are considered to be in government custody or control is often crucial to the outcome of an appeal.

The IPC held that political party records found in a government organization's offices are not outside the scope of the Act simply because they do not relate to the mandate or operation of the government organization. *If records are in the custody of the government organization, they are covered by the Act.*

Another appeal concerned records in the possession of a college ombudsman. Under the terms of his contract, the ombudsman operates in an independent and impartial manner and the college has no power to direct his activities on matters within his mandate. The ombudsman's files are to be kept secret and accessible only to him and he has his own record management and disposal system. The IPC held that the ombudsman's records were not in the custody or control of the college.

In several cases, the IPC re-iterated that promotion of informed choice in the purchase of goods and services is not relevant to the provision of *mailing lists* for marketing purposes. Individuals registering birth information, etc. would reasonably expect the information to remain confidential and disclosure would therefore constitute an unjustified invasion of personal privacy.

Each year, the IPC follows up to ensure *that government organizations have implemented the recommendations contained in the IPC investigation reports.* Of the total 53 recommendations for 1991, 43 had been fully implemented, 2 had been partly implemented and 2 had been replaced by satisfactory alternative controls. Six recommendations had not been carried out (reported as due to cost or other operational factors).

The IPC also conducts research on privacy questions, and advocates relevant legislative policy changes. Partial results of these actions are considered in other chapters of this report.

### 2.4.2 Judicial Review

Like decisions of other administrative tribunals, orders issued by the Information and Privacy Commissioner may be reviewed by courts on jurisdictional grounds. We mention one of the more interesting cases from the annual report ([10]).

The requester had been permitted to view records from the Stadium Corporation of Ontario, Ltd., the provincial government organization responsible for SkyDome, at the corporation's premises in 1988 and requested copies of certain pages he had examined. The corporation refused to provide him with the copies, on the grounds of various exemptions under the Act.

Later in 1990, the IPC ordered the corporation to disclose *certain records* found by the IPC not to be exempt. The appellant applied for judicial review, asking the court to set aside the interim order and provide *total access to the records*. He also claimed that the corporation had waived its right to invoke the discretionary exemptions after permitting him to view the records.

The Divisional Court [*Ken Rubin v. The Information and Privacy Commissioner of Ontario*, Court File No. 556/90] heard the case in January 1992 and *dismissed the application*. In concluding that the earlier access was not given *under the Act*, as was also interpreted by the IPC, the court found that the IPC was not in error in the given circumstances in the IPC legal interpretation.

The fact that the Privacy Act involves no penalties at all, as mentioned in the introductory part of the report, is surely one of the reasons, why the number of judicial reviews, which can only **review** the decision of IPC, is so low (e.g., 14 applications in 1992). Possible outcomes of a review are usually decisions granting or denying access to specific information.

## 2.5 Quebec

The Quebec government introduced **Bill 68** in December 1992, with the objective to exercise the rights conferred by articles 35 to 40 of the **Civil Code** of Quebec, concerning the protection of personal information. The Bill came into effect on January 1, 1994.

The Quebec *Privacy Commission* will play a lead role in overseeing administration of the act, investigating complaints and issue binding decisions, although questions of law and jurisdiction may be appealed to the courts. The Commission will, as with similar offices at federal or other provinces level, also have an educational mandate.

**This act is the first legislation in North America to regulate private sector collection, use and disclosure of client and employee personal data.**

Clients can not be denied goods or services for refusing to provide personal information unless the details were required by law or to fulfill contractual obligation, and consumers are also able to opt-out of telemarketing or mail solicitation and to find out how such businesses acquired their personal information.

As the article 38 states : "except as otherwise provided by law, any person may, free of charge, examine and cause the rectification of a file kept on him by another person with a view to making decision in his regard or to informing a third person".

The definition of record is as broad as in the Ontario Acts; but the definition excludes journalistic material collected, held, used or communicated for the purpose of informing the public. ([16])

In Quebec, every organization must state the purpose of personal data collection, *and must not use this information for other purposes* (Art. 4). The collection of information must be

limited to information related to the stated purpose; and no enterprise may, except where it has obtained consent of the affected person, use the material collected in a manner that was stated by the original purpose, and a file may not (subject to certain exceptions) be employed after the purpose for which it was created has been accomplished. (Art. 12)

**Information has to be collected from the affected person** (rather than third parties), except some defined situations, most notably when consent by the affected person exists or such collection from third parties is authorized by law. (Art. 6)

When establishing the file the collector of information must inform the affected person of:

1. the objective of the file;
2. the likely use and the types of persons who will have access to the information; and
3. the place where the file will be stored as well as any rights to access or correction.

(Art. 8)

The collector must arrange security measures to ensure confidentiality of such information (Art. 10).

Information must be up-to-date and accurate at the time when it is used as a basis for decisions in relation to the affected person. (Art. 11)

Except in certain circumstances, no possessor of personal information may communicate such information to third parties (Art. 13).

Bill 68 also contains *a provision affecting parties outside Quebec*. According to the Article 17, a Quebec business must take all reasonable steps to ensure that:

1. the information will not be used for a purpose not pertinent to the objective of the file;
2. the information will not be communicated to third parties, subject to certain exceptions
3. when address or phone lists are used for commercial or philanthropic solicitation, the affected persons must be given an opportunity to refuse such use of their information.

An interesting question is **to what extent the Quebec privacy legislation will apply to federally regulated businesses such as banking, transportation, or communications**, because then these would extend the level of privacy protection to other Canadians as well.

Specific provisions of the act deal with **credit reporting agencies, which must register with the provincial access and privacy commission and publish their activities** in the newspaper. The act sets out **fines for non-compliance ranging from C$1,000 to C$10,000**, depending on the offense.

## 2.6 ... Other Provinces

This section provides a brief overview of other provinces' jurisdictions; the approach is generally comparable to that of Ontario.

### Alberta

Legislation is expected to be enacted in spring 1994. Bill 61 - **Access to Information and Protection of Privacy Act** - received first reading in the Alberta legislature on April 26, 1993.

Concerning access to personal information, the act, relative to the information legislation in Ontario covers :

- fewer organizations falling within the definition of the act;
- fewer records falling within the scope of the legislation;
- broader exemptions from the general right of access ([16])

### British Columbia

The **Freedom of Information and Protection of Privacy Act** came into effect in October 1993. It also shows major similarities with the Ontario legislation. Some interesting differences include the following:

- public bodies are authorized to refuse to confirm or deny the existence of a record not only in situations when it is harmful to law enforcement, but also where the record contains personal information and where the disclosure of the existence of the information would be an unreasonable invasion of a third party's personal privacy;
- the law enforcement exception is expanded to protect sensitive law enforcement information in relevance to organized crime activities;
- the Attorney General's consent is required for the disclosure of law enforcement information that could be harmful to intergovernmental relations;
- B.C. has the first jurisdiction in Canada to cover as organizations falling within the scope of the act, self-governing professional bodies, such as the Law Society, the College of Physicians and Surgeons, etc.

The activities in British Columbia seem to have caught up with respect to legislative powers in the past years, and so the province joins advanced partners of Ontario and Quebec, in regards to information legislation.

### Manitoba

The Manitoba Act sets out the actions by which the privacy of a person might potentially be violated; these are, however, stated fairly generally, and the Act seems to need some sort of update with respect to recent technological changes.

**Northwest Territories**

The **Right to Information and Protection of Privacy** legislation has been proposed by the Minister of Justice in the Northwest Territories. An interesting issue on exercising residents' rights *in their language* is to be covered by this legislation. ([16])

**Saskatchewan**

The **Freedom of Information and Protection of Privacy Act** (Bill 70) and the **Local Authority Freedom of Information and Protection of Privacy Act** (Bill 71), received Royal Assent in June 1991; and were proclaimed into force in April 1992, resp. July 1993. Both pieces of legislation seem to be substantially similar to that of Ontario.

**Most of the other provinces do not have specific Information Privacy acts, and the relevant issues are sometimes covered by public government acts, access to information acts, etc.** .

## 2.7 ... and Private Sector ?

The Private Sector in the North America (except Quebec, as mentioned earlier in this report) *is not the subject of any special privacy legislation.* Various international experiences, and even requirements, demonstrate that legislation (or perhaps another assurance) should standardize the handling of personal information by private sector organizations. These are discussed in greater detail below.

### 2.7.1 The CSA Model Code

In order to meet some international requirements (mostly from European countries), and to assist Canadian private sector organizations, the *Canadian Standards Association* (backed mostly by Ontario businesses) initiated a development of **a model privacy code** as a minimum standard for private sector handling personal information, which (by [1]), "*holds promise for some meaningful privacy protection without resort to legislation*".

The CSA office declined to provide the author of this report with any information on the code development, as "*CSA shall not, without Submittor's prior written consent, voluntarily disclose information obtained by CSA in confidence ...*". It is questionable if development of the code which is demanded and done mostly for the public, should be subject of such restrictions, but this remains to be an issue of the CSA policy.

The members of the committee for development of a promotion of the model code (based on the OECD guidelines) represent finance, insurance, direct marketing, telecommunications, information technology, utilities, credit reporting, consumers and federal and provincial governments.

An important aspect is the overseeing mechanism, where the committee expects to make specific recommendations on several possible options for the registration of certifying industry specific codes ([1]).

### 2.7.2 OECD Guidelines

The Organization for Economic Cooperation and Development has developed a set of guidelines (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*), which may

be regarded as a code of fair data practices and can be briefly described as follows ([17]):

1. **Collection Limitation** : restricts the amount of data that may be collected based on its relevance;
2. **Data Quality** : the data must meet a certain standard of quality;
3. **Purpose of Specification** : the purpose of data gathering must be specified at the time of collection and notice must be given for additional uses;
4. **Use Limitation** : limits the use of the data to the purpose(s) for which it was collected unless notice has been given and consent obtained for additional uses;
5. **Security Safeguards** : must be set up to prevent breach of guidelines and to account for unauthorized access to the data;
6. **Openness** : stipulates that the nature of the data collected along with the identity and location of the data controller must be published in indices of a report with the applicable policies and procedures;
7. **Individual Participation** : the individual has the right to :
   - know whether data about himself is being maintained;
   - access the data in a reasonable time and manner in intelligible form without excessive charge; and
   - be given an explanation for in the event of denial to access and an opportunity to challenge the denial;
8. **Accountability** : a data controller should be accountable for complying with measures which give effect to the principles stated above.

Even without legislative sanctions, some private sector organizations have adopted all or some of the above principles (the Royal Bank and Bell Canada are said to endorse all of the guidelines, and the Canadian Bankers Association and Canada Direct Marketing Association some of them).

There are potential implications for information flow and trade between the EC and Canada because Canadian jurisdictions have not enacted legislation to govern the private sector in this regard (Canadian firms might be precluded from trading with the EC if the guidelines are not complied with - as suggested by the *draft proposal for a Directive by the Council of European Communities, released in July 1990.*) ([15]).

In regards to this fact, the Quebec jurisdiction initiative and emphasis on the private business information legislation might be viewed from a different view-point. The Quebec legislation covers a broader concept of privacy than the OECD guidelines, which are concerned primarily with information technology implications relevant to privacy rather than the concept of privacy itself. (These issues are in Europe covered by the *European Convention for the Human Rights and Fundamental Freedoms*, which Canada can not be a signatory of, due to the regional limits of the Convention).

Even the Department of Communications report ([19]) expressed disappointment with the Canadian approach : "*... in the ten years since their introduction, compliance within member countries has been uneven. In Canada, efforts by the private sector to implement this code [OECD] have been disappointing.*".

## 2.8 Across the Borders

The major development in the Canadian information privacy context is yet to be taken (as also the approach towards the OECD Guidelines was of no success) and may be expected to come into question with "Information Superhighway" issues (Section 4). One of the major pilots of European privacy principles was already outlined. We now look on the US legislation, namely the **Electronic Communications Privacy Act** of 1986, and excerpt a few articles of it.

Section 2511. **Interception and disclosure of wire, oral, or electronic communications prohibited**
(1) Except as otherwise specifically provided in this chapter and any person who

- (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

  .....

- (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

- (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

**shall be fined not more than $10,000 or imprisoned not more than five years, or both.**

Section 2701. **Unlawful access to stored communications**
(a) **OFFENSE** - Except as provided in subsection (c) of this section whoever

- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

- (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) **PUNISHMENT** - The punishment for an offense under subsection (a) of this section is (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain

- (A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

- (B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.
(c) **EXCEPTIONS** - Subsection (a) of this section does not apply with respect to conduct authorized

- (1) by the person or entity providing a wire or electronic communication service;
- (2) by a user of that service with respect to a communication of or intended for that user.

# 3 Policy Decisions Caused by Updated Technology

Technological developments, particularly of computers, communications, and miniaturization, have fundamentally changed the character of modern society. Concerns about information technology's influence on privacy are the subject of many more or less comprehensive and valuable articles, papers, and books. Particularly the use of wireless services and distribution of services and facilities, as well as their networking are the two main technological developments that have changed the nature of things. We briefly consider two of the new phenomena which have received a legislative attention.

## 3.1 Computer Matching

Computer matching involves computerized comparison of two or more systems of records or files. Databases are searched for the location of specific information (name, occupation, address, etc.) and then the computer examines this data according to a predetermined selection criteria. Data which meets this criteria is selected by the match as a *hit*. Matching is generally done by linking a single specific identifier (e.g., SIN) or a combination of several identifiers or unique data elements (optimally creating a key attribute). Examples of use might be checking for government employees (or taxpayers in common) above a certain income level against a database with records on welfare benefits; or, in the United States, males registered for the draft are checked against males over the age of 18 with driver's license ([20]).

**Supporters of computer matching** believe that all parties involved benefit from such activity. Benefits are considered to be both *quantitative* (e.g., monetary savings) and *qualitative* (e.g., improved law enforcement).

**Critics of computer matching** argue that benefits are overstated and unsubstantiated as the *lack of government overseeing* has meant *lack of reliable information* for computer matching. They are also critical of the exclusive use of information generated from computer matches to make decisions affecting the data subjects, and of the use of inaccurate information in matches. Various privacy advocates [6] report that use of computer matching results in :

- the data subjects' loss of control over their personal information;
- unlawful search and seizure;
- the presumption of innocence being turned into the presumption of guilt;
- lack of proper due process; and
- unequal protection under the law.

In general, most jurisdictions require that matching proposals be submitted to a data protection agency for review. Some of these agencies have the authority to suppress the proposals, while others just may only make recommendations.

### 3.1.1 Canadian Federal Policy

The Treasury Board of Canada issued a policy on Data Matching and Control of the Social Insurance Number in June 1989, which is based on the US government's 1979 computer matching guidelines, with basic principles as follows:

- **Public Notification** : A matching program should only be introduced after the public has been notified and given the opportunity to identify privacy problems;
- **Data Security** : The program should be conducted with safeguards on access to the data;
- **Exhaust Alternatives** : The program should only be introduced when there are no alternative, cost-effective means of identifying violators.

The Canadian federal policy, which applies to all government institutions listed in the schedule to the Privacy Act, requires such institutions to :

- assess the feasibility of the proposed programs *by doing a cost benefit analysis* of the impact of the matching;
- *notify the Privacy Commissioner* of new matching programs by providing him with copies of their assessments *60 days prior to when the programs are scheduled to begin*;
- subject the information gained by the matching programs to a *verification process* prior to using it for administrative purposes;
- account publicly for the matching programs (through the Index of Personal Information).

**The Privacy Commissioner may make recommendations to the heads of institutions concerning the matching programs**; only these (heads) or special authorities designated by them may approve matching programs.

## 3.2 Call Management Services

In November 1989, Bell Canada submitted an application to the CRTC (Canadian Radio-Television and Telecommunications Commission) for approval to introduce **Call Management Services** (CMS) with these four options :

- **Call Display** (also known as *Caller ID*) presents a visual display of the calling party's phone number, to the called party on a special type of phone with display.
- **Call Return** re-dials the last incoming call. This option incorporates a call scanning service. If the number re-dialed is busy, the service will continue to scan for 30 minutes.
- **Call Screen** re-routes up to 12 unwanted (a priori selected) numbers to a dead-end tape-recorded message at Bell Canada.
- **Call Trace** allows one to record and store details of the last incoming call. The stored information is available only to Bell Canada's Security Department and at the customer's request can be forwarded to a law enforcement agency for investigation.

The Caller ID allows display and collection of phone numbers without the knowledge or consent of the caller. Some businesses are using Caller ID to create telemarketing databases and mailing lists (through 'reverse' phone number directories). ([7])

It is necessary to point out that privacy is also based on the concept that information about an individual is his/her own, to communicate or not to others, as the individual determines.

CMS were approved by the CRTC in May 1990, despite numerous submissions from interested parties expressing concern over the privacy implications of CMS. In particular, Caller ID was viewed as an invasion of the caller's privacy, unless some way to block the transmission and display of the caller's phone number was made available *free of charge*. At that time, free call blocking was not endorsed by the CRTC (just 75 cents per call option with an operator assistance).

Following *additional submissions protesting* the May decision, particularly concerning the costs, the CRTC conducted another review of Bell Canada's application. In March 1991, the CRTC confirmed its original decision.

However, in May 1992, the CRTC **revised its decision and ordered Bell Canada to provide per call automated blocking free to those subscribers who request it**.

# 4 Information Infrastructure and Privacy

This section presents an overview of the U.S. initiatives known as National Information Infrastructure (NII), resp. Global I.I. (GII), with possible outcomes influencing privacy expectations; and Canadian (Ontario) issues.

## 4.1 National Information Infrastructure

Significant regulatory powers were delegated to an independent U.S. agency (the Federal Communications Commission) to work out the ideas outlined by the Clinton Administration about the NII. This expert body is expected to make technical decisions and to monitor, in conjunction with the National Telecommunications and Information Administration and the Department of Justice, changing market conditions. It is generally expected that the impact of the introduction of infrastructure based on communications technology, will be of the same magnitude as the introduction of printing technology.

The NII Task Force consists of 3 working groups: Infrastructure, Applications, and Information Policy. The Commerce Department has a much higher representation than the Regulatory Department, which means that economic concerns are very powerful in the debate.

Current estimates are that *$400 BILLION* are to be spent to "re-wire" the USA, in response to the NII initiative.

Information Policy is a balancing act among 4 issues: Property, Privacy, Public, and Government. Privacy and Public Access need strong advocacy to balance the dominant voices from corporations and government.

Alliances are forming to combine capital, avoid duplication of effort, and to move into the lucrative high-end consumer and business application markets. Cables are uni-directional but of higher bandwidth (e.g., good for video), while the phone networks have better switching (e.g., good for connecting). Public interest groups are concerned about the potential for monopoly

services. ([23])

It is interesting to note that the 24 countries of the OECD have only 16 percent of the world's population, but they account for 70 percent of global telephone lines and 90 percent of mobile phone subscribers. ([3])

Vice President Alan Gore also argues : "*The National Information Infrastructure, as we call it, will be built and maintained by the private sector. It will consist of hundreds of different networks, run by different companies and using different technologies, all connected together in a giant "network of networks", providing telephone and interactive digital video to almost every American.*", and
"*In a sense, the GII will be a metaphor for democracy itself. Representative democracy does not work with an all-powerful central government, arrogating all decisions to itself. ... The GII will not only be a metaphor for a functioning democracy, it will in fact promote the functioning of democracy by greatly enhancing the participation of citizens in decision-making.*" ([3])

Considering the above, we now consider one of the new issues of interest in the U.S., introduced recently by the Clinton Administration.

### 4.2 Clipper Chip

The Clipper plan, developed by the National Security Agency (NSA) in cooperation with the National Institute for Standards and Technology (NIST), was announced in April of 1993 by the Clinton Administration. It has been almost universally opposed by computer security specialists and public policy groups as well. A group of 38 of the U.S. leading computer scientists, computer security specialists and privacy experts have urged President Clinton that the Clipper program be stopped. ([18]) W. Diffie, R. Merkle, M. Hellman, R. Rivest, and others state in the letter to the President, "*The current proposal was developed in secret by the Federal agencies primarily concerned about electronic surveillance, not privacy protection. ... Critical aspects of the plan remain classified and thus beyond public review.*"

"If adopted, this will be the first partially classified federal information processing standard in history. The encryption method requires **escrowing user encryption keys with two trusted authorities**. The government has decided that the escrow agents will be the NIST and an arm of the Treasury Department." ([4])

Let us briefly overview and compare cited NSA advocacy (excerpts of The Wall Street Journal interview with *Clinton Brooks (quotations in italics)* of March 22, 1994) and opinions of some computer security specialists, namely **Lance J. Hoffman (quotations in bold)** ([4]), and privacy advocates.
*"the NSA is consumed with the 'equities problem'–how to balance privacy rights against the needs of law enforcement, national security, and private industry."*
*"... began discussion about how to improve computer security without making it impenetrable to police"*
*"The team decided against using a weak encryption code. ...it had to be good security."*
*"It would defeat the purpose [of the project] if we gave the knowledge of how the algorithm worked" to the public..."It was going to have to be kept classified. Otherwise engineers could use the algorithm to design computer-security systems that the government's encryption keys couldn't unlock."*
*"The only reason we're involved is that we have the best cryptomathematicians in the country."*

**"Burdensome and administratively less secure than some other encryption methods, key escrow technology is unlikely to be accepted by computer users who can get more secure methods elsewhere. Encryption is available around the world without the burden of key escrowing: Preliminary survey results from the Software Publishers Association revealed approximately 200 non-US and about 300 US-based cryptographic products".**

**"The administration did not reach out beyond the government to computer hardware or software manufacturers, to the telecommunications industry, to business in general, or to academe for advice during the planning of this initiative".**

**"Congress should mandate a serious, open, public review of cryptography policy and its implications for society".**

One of the very expressive and simple statements was posted by Steven W. McDougall, Collaborative Research Inc., in various privacy related newsgroups this March :

```
My concern isn't that the NSA is hiding something from us.
My concern is that the NSA will do exactly what it says:
Create a situation where the government holds the keys to all civilian
cryptography in the US.
I think that this is *bad*.  I don't want it to happen.
```

### 4.3 Canadian Superhighway

From the (`alt.politics.datahighway`) newsgroup, March 1994 :

CANADIAN SUPERHIGHWAY COMMITTEE TO MEET IN SECRET

So much for the future of democracy in the Great White North: It was recently announced that negotiations for the proposed Canadian data superhighway will take place in secret between representatives of establishment-owned Canadian corporate media, telephone and cable companies, with only token public representation. Canadian media is already tightly controlled by a few owners.

The Canadian federal government has finally announced that David Johnson, principal of McGill University, will be the chair of the Advisory Committee on the Information Superhighway proposed for Canada. The other 25 members are not yet announced and presumably have not yet been chosen by Mr. Johnson.

They will include representatives from major broadcasters, cable companies, consumer associations, business telecommunications users, labour unions and educators, according to a report by Southam News on Thursday March 17th.

Unfortunately, at the same news conference Industry minister John Manley said that the committee would meet in secret and that its final report would probably not be made public, although the Committee "would occasionally produce background and discussion papers that will likely" be made public, he said.

*End of citation*

As the federal committee is about to start its work (and thus **in secret**), the only related document available so far is the Report of the Advisory Committee on a Telecommunications Strategy for the Province of Ontario from a 'distant' past - August 1992. ([22])

This document in the chapter **Access to Information and Security of Privacy Guidelines** states the following example principles for a set of guidelines to balance the rights of the creator, the right to access public information and the right to individual security and privacy within the context of modern information and telecommunication technologies :

- privacy should be explicitly dealt with when considering the introduction of a new technology;
- no listening, viewing or recording without prior consent;
- fair warning before devices like speaker phones and caller identification are used;
- joint ownership of transactional data to insure joint agreement on any subsequent use of the data and any gains from its sale;
- those technologies altering privacy should bear the cost of restoring it;
- set a minimal threshold of privacy available to all;
- consistency of broad principles across all technologies;
- mechanisms for discovering violations and receiving compensations are required;
- intellectual property rights and the rights of the creator must also be recognized and guarded.

A set of access to information and security of privacy guidelines (legislation) should be developed within the larger information policy framework.

# 5 Summary

Canadian legislation, regulations and policies address different privacy issues, more in the *per item* context, i.e. usually with an *after - the - fact* approach, in order to correct and notify various outcomes of gradual involvement of information technology in our everyday lives.

The privacy acts, federal as well as the provincial, are applied to federal government, resp. provincial and municipal institutions only, and are in that context more or less extensions of access to information acts. They also

- do not penalize infraction against the law
  - while this is partially understandable, as fines would be applied from a government institution to government, but
  - the legislation also fails to penalize third party abuse of access privileges;
- specify excessively broad allowances for third party disclosures under them;
- state too broad (and thus not sufficiently specific and addressable) definition of *personal information*, which is then one of the causes of their generality - it is impossible to provide the same protection to data as a name or an address on the one hand, and to a private correspondence, health test results, etc., on the other hand. (A separation under categories *personal information* and **private information** might be quite useful).

On the other hand, the Information Privacy Commissioner's decisions are binding for future institutions' decisions; however, they are still subject to possible court review.

The more comprehensive European legislation, by providing a *tougher licencing approach* to data banks holding or expected to hold private information, assures that various *data protection commissions* ensure a public input into the initiative and government - independent control. Commissions have more regulatory power and the legislation *applies to both* **the public and private sectors**, which only the Quebec legislation covers in all of Canada (resp. North America).

*Building a new information infrastructure within the existing information privacy legislation framework almost surely will cause various discrepancies and problems for private citizens, industry, governments and public bodies, both Canadian and international.*

## Acknowledgements

I would like to thank Prof. George White and Prof. Paul Van Oorschot for their help and patience, as well as for their helpful suggestions, and Mike Just for his comments.

## References


[1] Privacy Commissioner/Canada. *Annual Report 1992 - 1993.* Canada Communication Group, 1993.

[2] Brad Evenson. Privacy under siege (5 articles). *Ottawa Citizen*, September 1993.

[3] Al Gore. On global information infrastructure. In *International Telecommunications Union Conference*. International Telecommunications Union, March 1994.

[4] Lance J. Hoffman. Who holds the cryptographic keys? The government key escrow initiative of 1993. *Computer Society News*, November 1993.

[5] Canada Houses of Parliament. *The Privacy Act.* Ministry of Supply and Services Canada, 1991.

[6] Information and Privacy Commissioner/Ontario. *Privacy and Computer Matching.* Office of the Information and Privacy Commissioner/Ontario, 1991.

[7] Information and Privacy Commissioner/Ontario. *Caller ID Guidelines.* Office of the Information and Privacy Commissioner/Ontario, 1992.

[8] Information and Privacy Commissioner/Ontario. Copying information to individuals inside and outside an institution. *IPC Practices*, July 1992.

[9] Information and Privacy Commissioner/Ontario. Third party information at the request stage. *IPC Practices*, October 1992.

[10] Information and Privacy Commissioner/Ontario. *Annual Report 1992.* Office of the Information and Privacy Commissioner/Ontario, 1993.

[11] Information and Privacy Commissioner/Ontario. Providing notice of collection. *IPC Practices*, July 1993.

[12] Information and Privacy Commissioner/Ontario. Responding to requests for personal information. *IPC Practices*, October 1993.

[13] Information and Privacy Commissioner/Ontario. *Smart Cards.* Office of the Information and Privacy Commissioner/Ontario, 1993.

[14] James E. Katz. Public concern over privacy: The phone is the focus. *Telecommunications Policy*, April 1991.

[15] Faxon Canada Ltd. *Handbook Exploring the Legal Context for Information Policy in Canada.* Faxon Canada Ltd., 1992.

[16] Shemin N. Manji. Recent developments in Canadian freedom of information law, survey of Canadian jurisdictions. In *Governmental Ethics Laws Annual Conference.* Information and Privacy Commissioner/Ontario, September 1993.

[17] J. Fraser Mann. *Computer Technology and the Law in Canada.* Carswell, 1987.

[18] John Markoff. US code agency is jostling for civilian turf. *The New York Times*, January 1994.

[19] Department of Communications. *Telecommunications Privacy Principles.* Communications Canada, 1992.

[20] U.S. Office of Technology. *Electronic Record Systems*. U.S. Office of Technology Assessment, 1986.

[21] Legislative Assembly of the Province of Ontario. *Freedom of Information and Protection of Privacy Act*. Queen's Printer for Ontario, 1987.

[22] Advisory Committee on a Telecommunications Strategy for the Province of Ontario. *Telecommunications - Enabling Ontario's Future*. Queen's Printer for Ontario, 1992.

[23] Sam Sternberg. Conference notes. In *British Columbia Information Policy Conference*. Vancouver, Canada, November 1993.