Privacy in Canada

Caryn Mladen

Contact: *Caryn Mladen*
Caryn@privaterra.org
416-816-7010

Contents

Overview

Privacy in Canada is at a crucial point — likely to change in the near future and already a hot topic for discussion, debate and press interest. While the Canadian public has been remarkably quiet about privacy matters, concerns about this important topic have recently come to public interest and have been the subject of much press and media.

In the last three months of 2002, several news media ran stories about new technologies for implanting tracking devices in humans, identity cards with biometrics and computer tracking systems, outlining only the positive benefits and ignoring privacy concerns. However, this bias is changing.

From January 18 to 28, 2003 there has been widespread press coverage about a new Royal Bank initiative that would result in personal financial information being shared across the Canadian/American border, a scandal involving gun registry documents discovered unshredded in a dumpster, the unexplained theft of a hard drive storing the unencrypted personal financial records of 180,000 Canadians owned by major insurance company, a prime time television show on Canada's national television network (the CBC) negatively portraying loss of privacy, and considerable newspaper, radio and television news coverage.

On January 28, 2003, the federal Privacy Commissioner presented his Annual Report. In it he criticized the systematic behaviour of the Government in using the September 11, 2001 terrorist attacks as an excuse to drastically diminish fundamental civil liberties and enact measures that put the existence of privacy in Canada at risk. Within days of its release, the Report and message were publicly supported by several advocacy organizations.

There has been no groundswell reaction by the Canadian public, and the eventual reaction of Canadians as a nation is unclear at present. Overall, most Canadians are, by nature, reserved and uninvolved politically. Besides, the increased press attention occurred very recently. Consequently there has not yet been time for a significant response. Few Canadians are meaningfully aware of privacy concerns and this, combined with the complex nature of most privacy issues (involving technology and philosophical issues that are generally ignored in everyday Canadian life) and the disinformation spread by parts of the government and law enforcement, makes for an unconcerned population.

Canadians have only an abstract concept of their own rights, freedoms and liberties, claiming to love them while being unable to articulate them clearly. In this way, Canadians resemble a less vocal American population. When our rights are infringed, Canadians are slower to complain and less likely to follow up than our American counterparts. Some of this is perhaps due to Canada's history — law came to Canada before the settlers rather than the reverse as is true in the United States. Some is due to our relationship with the United States – culturally Canadians feel connected to Americans, but overshadowed by them. There is always an assumption that Canada will follow the United States politically, economically and philosophically, but will do so in a less extreme way.

In privacy matters, Canada responded to the terrorist attacks by implementing some measures that are highly privacy invasive, but have rejected others. Serious debate continues to rage in Parliament over issues such as the implementation of a national identification card and extensive databases that would track the daily activities of Canadians.

Overall, the privacy environment in Canada is an odd mix.

On one hand, Canada is seen as a country that is world leader with strong privacy legislation, federal and provincial privacy commissioners overseeing laws and policies within the country, a vocal activist community, and Privacy Enhancing Technologies developed within its borders and by Canadians.

On the other hand, it has a relatively disinterested public that doesn't bother to learn how to protect its privacy or assert its rights. It supports a public sector that routinely becomes lax with regulatory privacy requirements and that allows usage of collected information to creep into areas for which it was never intended. Finally it has constantly expanding international obligations that might dismantle the fundamental principles upon which Canada's privacy laws are based.

Status of the Legislation

Canada is a Parliamentary democracy, with a constitutional division of powers between federal and the provincial and territorial governments. Parliament has two houses, the House of Commons and the Senate, and both must ratify a proposed law (known as a "bill") before it becomes enacted. Canada enacted its supreme law, the Constitution including the *Canadian Charter of Rights and Freedoms* (the "*Charter*") in 1982. While the right to privacy is implied in various sections, it is not specifically enshrined. Although privacy rights were specifically protected under the *Canadian Human Rights Act*, this legislation was superceded by the *Charter*.

The Constitution divides powers between the Federal government and the various ten provincial and three territorial governments, but many sectors and matters fall into both jurisdictions. For example, corporations can be regulated either federally or provincially; the *Bank Act* is a federal statute but provinces also regulate financial institutions such as credit unions and insurance companies. Privacy is regulated both federally and provincially, and regulatory provisions are contained in a variety of laws in different sectors as well as overall privacy-specific legislation.

The Canadian judicial system is based on common law, except in the province of Quebec, which uses the Civil Code, a historical artifact from its past as a French colony. The province of Quebec is an exceptional legal entity. While it is subject to the Constitution and *Charter*, Quebec conducts its affairs differently than the rest of Canada. It was the first to enshrine privacy protection in its laws and continues to extend the application of the right to privacy.

The types of laws in Canada can be divided into four branches:

- **Criminal** – Provincial and Federal court levels can be appealed to the Appeals Courts and then to the Supreme Court of Canada. Police investigation powers are balanced by various rights of the individual, including the right to counsel and the fundamental rights and freedoms enshrined in the *Charter*. Privacy protections are also written into the *Criminal Code* however breaches of privacy are generally not considered a criminal offence. Instead, individuals must sue for breach of privacy in civil court, or work with the Privacy Commissioner to have the matter referred to the Federal Court. The only legally recognized requirements for Canadians to identify themselves to police are if arrested, conducting a licensed activity such as driving.

- **Civil** – including contract and tort law, civil law encompasses disputes between private entities, however individuals can sue government entities for breaching their rights. Court documents are open to the public unless a special "gag order" is imposed by the presiding judge. In British Columbia, Manitoba, Newfoundland and Saskatchewan individuals can sue other individuals for invasion of privacy.

- **Public** – including administrative tribunals and immigration law, public law is quasi-judicial review by state entities.

- **Family** – this branch concerns issues of marital law and the welfare of children. The suppression of making information relating to minors public is relatively standard procedure, although debated by some people as being too lenient on youthful offenders.

Rooted in Canadian law is the concept of "reasonableness" which is used as an over-riding principle in much legislation including the *Charter*. It is used in both judicial review (judges must consider what a "reasonable" person would have thought, done and concluded) and in creating exceptions (the law applies except when its application would be unreasonable based on the circumstance). What is considered reasonable varies depending on the individual, the particulars of the case and the attitudes of society at a particular time.

Tied to the concept of reasonableness is the "proportionality" test whereby judges balance the rights of the individual against the purposes of the law. Section 1 of the *Charter* "guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."

Federal Legislation

Privacy Act

The federal *Privacy Act* was adopted in 1982 and came into force on July 1, 1983. This Act regulates the collection, use and disclosure of personal information by federal government departments and agencies. The Act outlines a basic respect for privacy principles and gives Canadians the right to access and correct their personal information held by these federal government organizations.

Exemptions to access exist for national security purposes or if such access would compromise an ongoing criminal investigation. In these instances, citizens may not even know that the information has been collected. These instances are highly discretionary and it is easy to stamp an entire database with the phrase "national security" with little audit or oversight.

Personal Information Protection and Electronic Documents Act ("PIPEDA")

The fist stage of this Act came into force on January 1, 2001, setting regulations as to the "collection, use and disclosure" of personal information for the federally regulated private sector, and for personal information sold interprovincially. As of January 1, 2002, the personal health information collected, used or disclosed by these organizations is also covered. As of January 1, 2004 the scope of the Act will broaden to include all information collected, used or sold in course of commercial activities. At that time, any provincial governments that have not enacted provincial privacy laws that are substantially similar to *PIPEDA* will be regulated by the federal law.

Regarding collection, use and disclosure of personal information, *PIPEDA* requires informed prior consent, collection by fair and lawful means and for clearly stated purposes, usage only for stated purposes, and timely destruction of personal information after the purpose for which it was collected is completed. It also requires that commercial activity cannot be dependant upon provision of personal information. Exemptions exist for necessity and law enforcement, as well as for privately held information about friends and family, and information used for journalistic, artistic or literary purposes.

Individuals have the right to access and request correction of this personal information, and to expect the collecting entity to appropriately secure their privacy. Exceptions exist for national security, solicitor-client privilege and threats to the safety of others.

Access to Information Act

Enacted in 1985, this Act regulates the access to publicly held information and is overseen by an Information Commission. It is an odd overlap of similar functions that has been resolved in several provincial jurisdictions by combining the roles and creating an Information and Privacy Commission.

Pro-active and Reactive Legislative Development

The enactment of privacy legislation in Canada has been partially pro-active and partially reactive. The *Privacy Act* was proactively undertaken, emerging from debates undertaken during the passage of the Constitution and the *Charter* in 1982. While privacy rights failed to be enshrined in the *Charter*, a year later the *Privacy Act* came into force.

In 1995, the *European Union Privacy Directive* ("*EUPD*") was introduced, which would prohibit EU members from transferring personal data to non-EU countries unless "adequate" legislation existed in that second country to protect the privacy of the individual. In Canada, only Quebec had already enacted such laws so, fearing trade barriers, Canadian private commercial and public interests developed the Canadian Standards Association (CSA) *Model Code for the Protection of Privacy* in 1996, which led to the passage of *PIPEDA*. The *EUPD* went into force in 1998.

Like *PIPEDA*, the Model Code addresses the ways in which organizations collect, use and disclose personal information. It also addresses the rights of individuals to access and correct their personal information.

The *Model Code*'s 10 principles are:

1. Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

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

4. Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be

retained only as long as necessary for the fulfillment of those purposes.

6. Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

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

8. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Provincial Legislation

Privacy rights have been codified in several laws and Quebec currently has the best functioning privacy protection in the country.

The *Quebec Charter of Human Rights and Freedoms* enshrined the right to privacy for Quebec residents in 1975. Quebec's Civil Code was amended in 1991 to systematically ensure privacy protections were included and guaranteed for judicial matters. In 1994, the province passed *An Act Respecting the Protection of Personal Information in the Private Sector*, which comprehensively regulates the collection, use and disclosure of personal information held in the private sector. This Act also gave individuals the right to access any personal information about them held by a Quebec-based business.

The other provinces and territories have enacted or are in the process of enacting freedom of information and privacy legislation relating to the public sector, but only Quebec has passed legislation that is substantially similar to *PIPEDA*, covering privately-held personal information. Provinces that have enacted such legislation by 2004 will be exempted from the application of *PIPEDA* to provincially regulated commercial activities, and will be able to regulate them at the provincial level. Canadian personal data protection legislation includes a general right to access and correct personal information, and proscribes the use, disclosure and sale of such information without permission, subject to specific exceptions. Alberta and Manitoba have also enacted medical privacy legislation, and Ontario and Saskatchewan are attempting to do so.

Other Laws

Several other laws at the federal, provincial and even municipal level address the protection of privacy, and administration of personal information. These may be sector specific, such as banking and health-related laws. Or they may be more general, such as consumer protection laws and tort laws. There is little uniformity in such laws as there was no privacy mandate underlying their creation.

Judiciary

The judicial branch of the government is independent of the legislative (or law-making) branch. The courts have the authority and responsibility to interpret and enforce laws. In doing so, they have the authority to strike down legislation if it is determined that the law conflicts with a higher law, specifically with the Constitution and the *Charter*. Courts may impose judgments by requiring compliance, setting fines, requiring payment of one party to another, and imposing prison or jail sentences.

The Supreme Court of Canada has recognized that "privacy is at the heart of liberty in a modern state" and recognized three "zones of privacy", being territorial, personal and informational. The Court has not yet considered whether the tort of privacy invasion exists, however it has been recognized in various provinces.

The Privacy Commissioner may refer matters to the Federal Court. This provision is being challenged in the Kelowna case described below. One difficulty in taking privacy matters to court is dealing with remedies. It is difficult to quantify the value of personal privacy and few cases have been heard on this matter. Generally, it is not considered financially worthwhile to bring a case of breach of privacy to court, unless the case is a class action, in which many individuals come together to sue an infringing defendant in a civil case.

For an individual to bring such a case, that individual would need to weigh the costs of legal fees and lost income caused by time off work against what is likely to be a relatively low financial settlement, *if* the case is won. As well,

the individual would have to explain to the court exactly what occurred, including providing details of the privacy breach, effectively exposing one's private information to the public on an even larger scale. Because of the understandable reluctance of individuals to pursue their privacy rights in court, there is a danger that the *Privacy Act* will be hardly used by the public and it will gain a reputation in political circles as being irrelevant.

International Laws

Canada is a member of the *United Nations and a signatory to the Universal Declaration of Human Rights*, which states in Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Canada is also a member of the Organization for Cooperation and Development (OECD), and in 1984 signed its *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*. The *Guidelines* outline fair information practices.

The European Convention on Cyber-Crime

Canada signed a Treaty to ratify this Convention and is in the process of attempting to pass legislation necessary to ensure compliance with its terms. These so-called "Lawful Access" measures are discussed in detail in the section "International Obligations".

Interpretation of these obligations and guidelines has varied amongst countries. Indeed, some consider the UDHR to be a mockery since it is not applied in many parts of the world and little is done to enforce it. The Lawful Access provisions initiated a swift and concerted backlash by Canada's privacy activists. Canada's positive reputation for fair information practices has been relatively deserved, but is at risk if presently debated measures are made a reality.

Privacy Commissioners

The position of federal Privacy Commissioner was established by the *Privacy Act*. The PC acts as an ombudsman, mandated by Parliament to oversee and defend the privacy rights of Canadians. Specifically, the Privacy Commissioner is responsible for oversight of the *Privacy Act* and *PIPEDA*, ensuring that personal information is collected, used and disclosed only in a manner that is responsible and transparent, and that regulated entities are held responsible for their activities. The Privacy Commissioner has specific rights and duties of investigation and report, but he cannot make law, order compliance, or pass binding judgments on privacy matters. These powers remain with Parliament and the provincial and territorial legislative houses, and with the courts. The Privacy Commissioner has the power to make matters public, and to take matters to the Federal Court of Canada.

The Privacy Commissioner is also required to research, educate and promote privacy issues in Canada, as well as to make reports directly to the House of Commons and to the Senate.

The Privacy Commissioner is responsible for matters of access to information and has the duty to intercede on behalf of the public in matters of privacy. The Privacy Commissioner has powers of investigation and report, but no power to enforce or impose remedies or penalties. Indeed, the role of Privacy Commissioner is minimally defined and highly discretionary. The actual activities of Privacy Commissioners are generally determined by the personality of the individual.

Each province and territory has a similar entity, that may be called an Information and Privacy Commissioner, a Commission d'accès à l'information, or similar title. The mandates, duties, powers and responsibilities vary somewhat from province to province and territory to territory, but all are substantially similar.

Enforcement

While Canada has adequate privacy legislation, problems remain in the administration and enforcement of this legislation. The recent Annual Report of the PC demonstrated numerous instances of public and corporate entities ignoring or being unaware of privacy concerns. While they are subject to the *Privacy Act* and *PIPEDA*, these are not their focal regulatory legislation. Further, the oversight, audit, enforcement, remedies and penalties associated with violations of these Acts are vague, discretionary and minimal. Hence, few such entities bother to familiarize themselves with the requirements of the Acts.

While the PC has the duty to intercede in privacy matters, he has no substantive powers to enforce adherence to the law. Indeed, government entities have been openly hostile to involvement by the PC or simply refused to take any advised action even when the advice of the PC has been couched in the strongest terms. In his recent Annual Report the PC stated that "governmental disregard for crucially important privacy issues is…becoming systemic" and warned that if the situation continues "privacy protection in this country will be progressively weakened, and

worse and worse intrusions will be inevitable."

Examples demonstrate that the issues involved are widely encompassing and non-trivial, including:

- Requests to limit the uses of the Canada Customs and Revenue Agency's airline passenger database (that the CCRA has decided to retain for six years and share with other governmental departments) has been refused without explanation or specific justification despite the fact that the Minister in charge has been made aware by prominent legal experts that the database undoubtedly contravenes Charter rights.

- The federal government is attempting to increase state powers to monitor communications through lawful access provisions in accordance with European Convention on Cybercrime, the treaty for which was signed by Canada prior to any consultation by the Canadian public. Public outcry from activist organizations resulted in some consultation and almost universal condemnation from privacy commissioners and organizations alike. Yet, the government has not responded to concerns about whether such powers are necessary to achieve the goal of reducing cybercrime, and whether the threat to fundamental rights is worth any perceived benefit.

- Provincially, the PC initiated action in July 2002 in the Supreme Court of British Columbia in the city of Kelowna to declare public video surveillance unconstitutional. Instead of participating in the public determination of the issue, the BC government challenged his right to take this action, trying to prevent the case to be heard on its merits. The challenge is before the courts now.

This disinterested response to privacy matters is not new. In 1987, Parliament produced *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, a comprehensive review of the *Privacy Act* and the *Access to Information Act*. *Open and Shut* made more than 100 recommendations but none became law although some did appear as policy directives.

In assessing Canadian privacy law, it is important to recognize that most of it is relatively new and poorly understood. Some of the concerns discussed in this paper may be corrected over time. Further, the behaviour of the government in ignoring studies, reports and the emphatic messages of the PC are not peculiar to privacy law and policy. Indeed, it is widely recognized that the Canadian government has frequently spent several years and millions of taxpayer dollars on investigations, Royal Commissions, and other reports, only to disregard them once they are completed.

While several Canadian laws address privacy, the application is often sloppy and non-uniform. Overall, the government recognizes privacy as a concern, but not a matter of significant importance. When weighed against almost any other law or issue, the other law will be given primacy and privacy rights are routinely infringed.

The State of Privacy Technology in Canada

Privacy advocates generally agree that technology itself cannot be considered the saviour for privacy. Rather, technology can be privacy *enhancing* or privacy *invasive* depending on its application — the technology itself is privacy neutral.

Another recognized aspect of technology is that it changes rapidly. Because of this it is important to draft legislation that is technology neutral. Any legislation that focuses on the working of a particular technology will soon be obsolete.

Privacy can be divided into four different aspects:

- **Personal information privacy** — facts about an individual that can be used to identify him. These may be kept in databases, files or embedded on so-called "smart" cards;
- **Bodily privacy** — biometric information such as blood samples and DNA;
- **Privacy of communications** — spoken, written or digital communications, and this may include identifying information that is contained within the content; and
- **Territorial privacy** — the right to be left alone in one's physical space, such as the home or office.

Typical technologies used to protect (or exploit) privacy include public key infrastructure (PKI) and biometrics including fingerprints, iris scans, DNA samples, facial recognition, and more. These technologies are not unique to Canada so this report will discuss only the specific application of the technology within the country, and not the background on how the technology works or is developed.

Identification Technology

Identification cards are used for two purposes — access and entitlement. Off-line cards with biometrics (that are not connected to a central database) are useful for access purposes. The issue this technology seeks to answer is: can this person enter, leave or have access to certain information? In this case, the identification technology acts as a lock that only the specific individual can open. However, any time the information must be processed by a particular government department or other organization, another system must be used. If others have access to the information, then the system is not locked.

On-line cards work with databases and these are used broadly in Canada. At present there is a public debate raging between government ministers and privacy advocates over a variety of measures including a national identification card, an airline database, and other measures. We discuss the policy implications of these later in the report.

The False Promise of Identification

When identification is necessary, it is important to ensure the system is authoritative, accurate and fraud-resistant. The problem with any identification system is that, typically, the creation of one document is dependant on the accuracy of other documents that are presented. To obtain a driver's license, you have to show your birth certificate and SIN card, but neither of these has a photograph so it would be trivial to obtain a fraudulent driver's license using the cards of someone else. The driver's license, on the other hand, contains a photograph and is the most frequently used form of identification in Canada.

The first question to be considered when designing a technology to minimize privacy invasiveness is as follows: is there any need for personal identification for a particular transaction to take place? In most commercial situations, identity is irrelevant. A vendor only needs to know if an individual can pay for the product or service. If the individual wishes to use credit, then identification becomes an issue to allow the vendor to track the individual if the credit proves to be fraudulent. In cases of returns of products, the vendor similarly does not need assurance about identity. He only needs assurance that the product being returned was purchased from the particular store (or other retail or commercial outlet) and is being returned in good condition according to the particular return policies of the company.

False Identities

False identities are frequently used, both online and in person. This is not a Canadian phenomenon, as it occurs throughout the Internet and in several other countries. When asked for identification to fulfill a particular transactional requirement, many people invent an identity and use it. In stores, few clerks have any interest in verifying identity. Indeed, when asked why the information is needed, most will have no explanation. It is part of the system and they have been told to ask for identification. Sometimes, it is not necessary for a transaction but sometimes it is required. However, it is rare that *proof* of identity is required in such circumstances.

Online, estimates of the percentage of false identities

used range from 40 percent to over 85 percent. While this behaviour might be considered fraud, the very popularity of it makes it less likely that fraud can be proven. With such high percentages estimated to be using false identities, it is difficult to prove that one had a reasonable expectation that the identity was correct. A specific exception to this argument exists in situations where individuals use the identity of another or falsify their identity to obtain financial gain.

Identification When Crossing Borders

It is necessary to prove one's identity for border crossing because of the demands of both security and immigration. Canadian citizens are permitted relatively easy access to many countries, especially the United States. However, it is insufficient to simply show yourself to be a Canadian citizen to enter. Your identification must be cross-checked with other databases to ensure you are not a wanted criminal or otherwise dangerous person.

Also, your identity must be recorded along with the date of your entry to allow Immigration and Naturalization Service (INS) agents to attempt to track and deport you if you remain in the United States longer than you are permitted to stay according to the law. Of course, individuals that use a fraudulent identity to cross the border are unlikely to continue using it after they have entered the country.

The Canadian Immigration Minister is actively and forcefully lobbying for the creation of a National ID card with embedded biometrics. After listening to him discuss the proposal, it becomes evident that he does not understand the technical details and logistical implications of using biometrics. Indeed, he may not even have a clear understanding of the basics of biometrics. He suggested calming privacy concerns by using an off-line biometric system, where a fingerprint or iris is checked against a coded sample kept on the card, and not checked against a centralized database. The obvious problem with this method is that it would not work to diminish fraud so it would not be effective as an identifier.

Social Insurance Number

Canada uses a national level social insurance number (SIN) scheme used for the administration of Canadian social benefits. As we discuss later in this report, there are specific uses of this number required and limited by law. However, many corporations request this number in order to perform credit background checks for establishing new business accounts and for future identification purposes. Policy issues relating to the SIN are outlined later in this report.

As a simple technological marker, the SIN is privacy invasive by design. The number assigned to an individual is determined based on generic background information about the individual including originating geography within Canada (province, territory or region), immigration status and other factors. While the system for deciphering such information is not widely known, Web sites easily located through a Google search explain the general algorithm.

Common Abuses of the SIN

There are almost 4 million more active SINs than there are people in Canada. Using a Canadian population estimate of 30 million people, these "extra" SINs mean that over 13 percent of all active SINs are somehow duplicated or fraudulent.

It is relatively easy to fraudulently obtain a SIN and common abuses of the SIN include illegally obtaining government benefits, insurance, and credit cards. Further, SIN fraud investigations are relatively weak and ineffective. These investigations are undertaken by the SINs regulatory body (Human Resources Development Canada) instead of a law enforcement agency and the maximum penalty for SIN fraud is a $1,000 fine and one year in prison.

Biometrics

By definition, biometrics is the study and statistical analysis of biological data. In security circles, biometrics is considered any technology that automatically authenticates an individual's identity based on a measurable (and hopefully, unique) physical trait such as a fingerprint. The use of biometrics in Canadian society is widespread and becoming more and more prolific.

Canadian law enforcement agencies make extensive use of finger, face and distinguishing marker biometrics (such as tattoos, scars and birthmarks) in the processing of suspects and convicted criminals to help establish matches for previous and future crimes. Recent software developed for law enforcement will soon allow these agencies to employ facial recognition in identifying known criminals, suspects or *persons of interest* with increased efficiency in ongoing surveillance and investigation activities.

Biometric databases have been incorporated for social benefits. An example of this is in the Greater Toronto Area in Ontario where biometric information is used to help reduce multiple access to the welfare system. Interestingly, due to pressure from the Ontario Information and Privacy Commissioner the biometric samples obtained under this program must be destroyed after use. While in

use, it is stored in an encrypted database that is not shared with any other agencies unless a court order or warrant is produced. Furthermore, the biometric information contained within the database has been designed so as to not allow the reconstruction of the original biometric marker. Thus, the information on the database cannot be reverse engineered to allow law enforcement or other parties to use the information to identify individuals.

In recent cooperation with the United States Immigration and Naturalization Service (INS), Canada has installed hand geometry biometric systems in two international airports to allow a quicker immigration clearance process. Another pilot project has also been undertaken at the Thunder Bay International airport to use facial biometrics to verify passenger identity quickly. Canada Customs and Revenue Agency (the former Revenue Canada) is also expected to contract the installation of KIOSK systems equipped with iris based biometric devices in eight Canadian airports. The system requires a yearly fee and a background security check. Further, users would be subject to random inspections, although users are promised faster processing through customs as a benefit of using the system.

The iris scanner equipped KIOSK is not a lucrative contract (approximately $10 million) given the wide extent of the rollout but it does provide a significant opportunity for Canadian biometric companies to better position themselves for introducing similar systems in other developed counties. In all, biometric systems for a variety of government agencies have become popular in recent years. They are being introduced with tight timetables and contractors are likely to see larger budgets available for these systems in the future.

Emerging Biometric Immigration Systems

Since June 2002, new immigrants to Canada have received a Permanent Resident Card containing biometrics and other security features. As of December 31, 2003, the new card is a necessary document for every permanent resident re-entering Canada by commercial carrier (airplane, boat, train and bus) after international travel.

The Permanent Resident Card has a laser engraved photograph and signature, as well as a printed description of the physical characteristics (height, eye colour, gender) of the cardholder. The Card's optical stripe will contain all the details from the cardholder's Confirmation of Permanent Resident form. This encrypted information is only supposed to be accessible to authorized officials (such as immigration officers) to confirm the status of the cardholder. The card's optical stripe is more advanced than a magnetic stripe (commonly used on bank cards) both in terms of information storage capacity and security of information. Much like a commercial compact disc, it is virtually impossible to change, erase or add to the information already encoded on the optical stripe. These features are promoted as making the card one of the most fraud-resistant documents in the world.

Forensic DNA Analysis in Law Enforcement

In 1998, the DNA Identification Act established a national DNA data bank, consisting of a crime scene index and a convicted offenders index, to be maintained by the Commissioner of the RCMP. Canadian legislation limits the use of DNA testing in establishing evidentiary information in certain Criminal Code offenses. Unlike other jurisdictions, such as the United States, the testing is limited to only the suspect, and may not be extended to relatives of the suspect when the suspect is not available.

Furthermore, current DNA testing is not used in screening or monitoring but only in matching a suspect to a crime scene. If the accused is acquitted, the charges are withdrawn or the prosecution enters a legal "stay", the genetic sample and test results are legally required to be destroyed. Whether this destruction of collected DNA actually occurs is another question. In the past, there have been scandals in Canada relating to police and other governmental databases that were supposed to have been destroyed but continued to be used for many years.

DNA testing conducted in Canada is limited to identifying DNA markers that are not associated to known genetic diseases or disorders, or to physiological characteristics such as hair color. The current testing process is also limited by the quality of the samples provided, as low quality or quantity samples will provide poor matching results.

Database Technology

Databases are used in all levels of government, as well as in private businesses. There are centralized Canadian databases operated for purposes such as social insurance; provincial databases for purposes such as administering health insurance; marketing databases; customer loyalty databases; and many other forms of databases.

Law Enforcement DNA Database

The Canadian federal law enforcement agency, Royal Canadian Mounted Police (RCMP) maintains a three million dollar a year DNA sample database. The database is intended to help law enforcement agencies solve crimes

from the past, present and future by comparing stored DNA samples to crime scene samples.

Healthcare Databases

Each Canadian province and territory maintains sophisticated and detailed medical databases intended to provide easy and reliable healthcare information to help medical professionals aid any patient with proper diagnoses and treatments. Also, third parties such as insurance companies, often access these same systems to assess a prospective client's eligibility for an insurance policy. Insurance companies are able to access this information only under a disclosure agreement signed by the client.

A common problem of this process is due to the inflexibility of these records to be corrected after a dishonest health care professional makes fraudulent claims. This is described in more detail in the section of this report on Medical Privacy.

Data Leakage

Recently in Saskatchewan a hard drive was stolen from a company that handles government records. The theft represents Canada's largest security breach to date as the hard drive contained extensive amounts of personal information. The act itself was apparently little more than a case of petty theft as the individual (an employee at the contracted company) had only intended to acquire the hard drive for personal use and only fragments of the original data was recovered from the stolen hard drive. The original files were largely overwritten with other data. Law enforcement officials have stated that they are confident that the information was not used illegally and that the data device was never publicly accessible.

However, officials are unable to confirm if any of the original data was copied from the hard drive prior to the device's physical recovery. An investigation has been launched by the government, a class action lawsuit is being organized and the culprit is facing charges for theft under $5000. Since there is no evidence that the data was stolen (rather than just overwritten), more serious *Criminal Code* charges could not be laid against the individual.

In the mid 1990s, the half-burned records from a large Canadian hospital were found floating by a nearby coastline, the apparent result of a failed attempt at destroying the records by burning them on a beach. This was apparently not the normal practice for destroying old documents but the individual normally responsible for the purging the information was not available and another employee at the hospital assumed the responsibility. The result of poorly established and enforced protocol was ultimately to blame.

Private and Business Use

Unregulated Cryptography

There is no law in Canada prohibiting the use of encryption for personal information being transmitted domestically or internationally. The Canadian government does not maintain policies to acquire backdoor keys to any commercially or privately designed digital encryption technologies in use currently. Canadians are however not well educated on average in protecting their personal information from third party attempts to acquire potentially valuable information from insecure transmissions.

Invasive Network and Wireless Computing

Security and privacy for home computers and home wireless networks are often not protected from aggressive or malicious third parties who are attempting to track the user's actions or acquire valuable information about the user. In most Canadian cities, a laptop computer equipped with a wireless networking card can access and use any number of open and insecure wireless LAN home networks when roaming neighborhoods. Currently, there is little large-scale organized effort to educate the public about these vulnerabilities.

Canadians do, nevertheless, have access to any number of modern software and hardware solutions to provide security and privacy for personal computing needs. Widespread use of network security systems in corporations and information technologies in general are very common in most commercial settings with widespread training. In the end however, network security and privacy is the responsibility of the individual entity.

Privacy Versus Security Paradigm

Within Canada, some discussion has begun about challenging the old paradigm of privacy versus security as "a zero-sum equation". It is often stated by politicians that we must "give up our privacy in order to be safe". Some emerging technologies, it is argued, could provide both privacy and security to a system if the planning is conducted with both goals in mind.

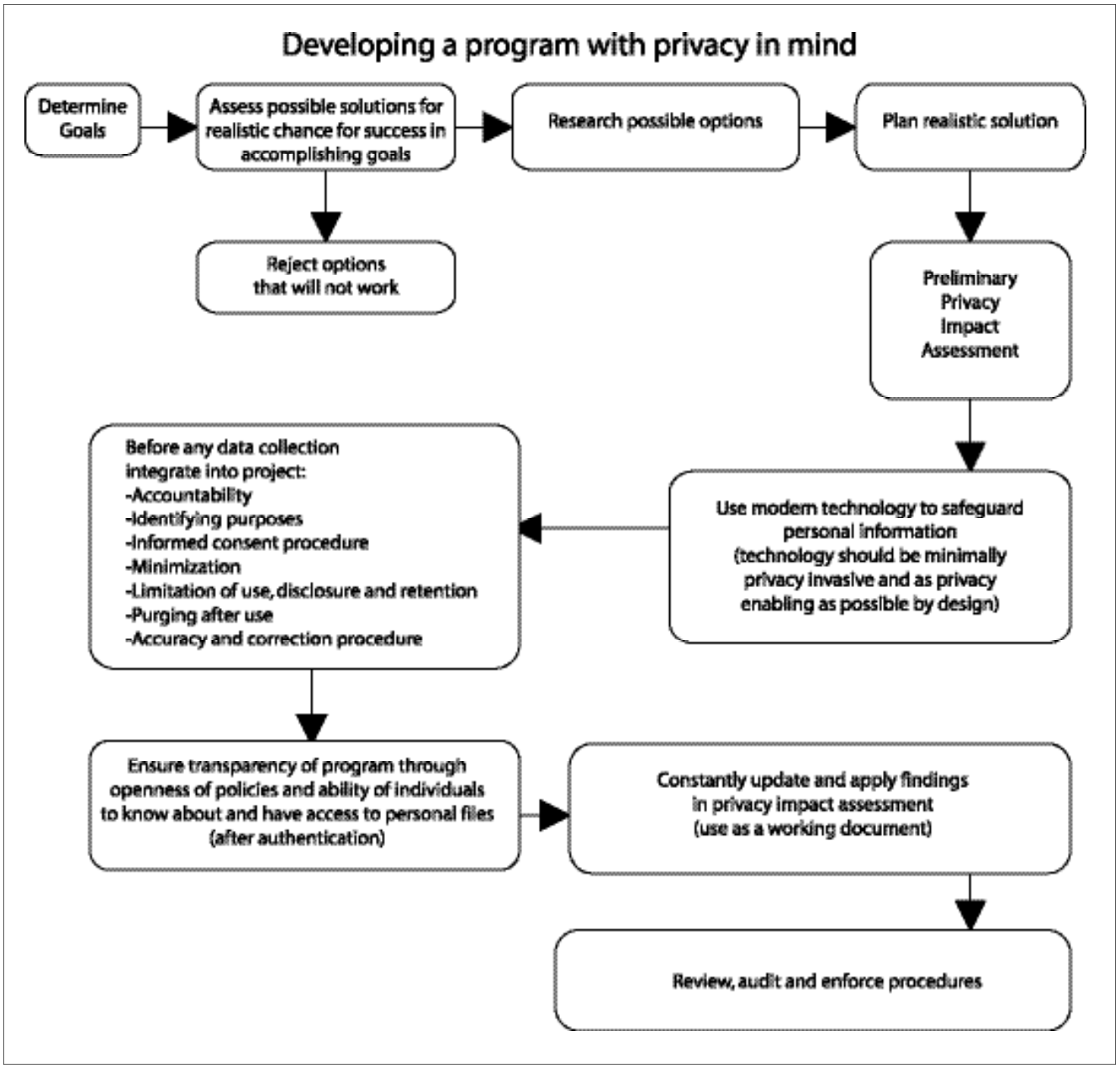
A recent paper by Ontario's Information and Privacy Commissioner has proposed the use of newer 3-D holographic imaging using millimeter wave scanning techniques at airport terminals to check for concealed weapons

while not viewing the naked body itself. Traditional airport body scanners outline your physical body and show any other non-physical elements (such as weapons). The 3-D holographic scanners only show the non-physical elements. Since the goal is to screen for dangerous tools or contraband, there is no need to observe the shape of a person's body. It should be obvious to choose the less privacy invasive scanner, but modern culture suggests we are safer the more we know about everyone else, even if that information is irrelevant to our purposes.

Principles

The principles relating to privacy technology are simple and developers consider them rather obvious. Recognizing this, it is surprising how rarely privacy issues are even considered in the design of systems.

Principle 1: Know your goals — Too often, the ultimate goals of a policy are forgotten in the rush to build a system. People designing border-crossing systems need to remember that the goal of these systems is to allow entitled people to cross the border and to prevent anything dangerous from crossing the border with them. Of course, this brings up the possibility that government actors may have other goals than those they state. In designing border-crossing systems, it is important to know if the true motivation of a government is to secure the public, to protect fundamental liberties or to track the movements of its citizens.



Principle 2: Create solutions that incorporate only what is necessary to achieve those goals — This principle flows from the first Principle. If one doesn't need to confirm identity for a particular transaction to be valid, then one should not require identification.

Principle 3: Consider the privacy implications of a system or technology – Whether through a privacy impact assessment or simple common sense, it is necessary to understand exactly what the proposed measure will do, both now and in the future. This is a typical problem with politicians suggesting the implementation of technology they do not understand.

Principle 4: Use privacy enhancing technologies to protect privacy whenever possible — When two technologies accomplish the same goal, choose the one that best enhances privacy. For example, a 3-D holographic imaging scanner used at airports, is an example of this choice.

Principle 5: Use policies that support the privacy enhancing nature of the technology — this is discussed in detail in other parts of the report.

Principle 6: Make privacy an on-going part of the project. As systems, goals and technology changes, it is necessary to reconsider all elements of the project, including privacy.

Sectors

The players in the Canadian privacy environment can best be examined in four sectors: the Private Sector; the Activist Community; the Government and Public Sector; and Business and Industry. Each group plays a crucial role in the development, implementation and evolution of privacy in Canada. For each sector, the impact of privacy laws, initiatives and technologies is significant.

The Private Sector

To consider privacy in terms of the general public in Canada, first it is important to understand what Canadians consider privacy to be. This can be a challenge because few Canadians think about privacy as a concept and only notice it when something happens that affects them personally. Do Canadians value privacy? The lax attitude toward privacy may simply be the result of never needing to question its existence. This is likely to change in the next few months and years as more privacy-invasive technologies and policies are developed and deployed in the country.

Generally, Canadians recognize the importance of a general privacy principle, but also acknowledge the need for exceptions to be dealt with on a case-by-case basis. Specific groups are singled out as requiring special privacy laws and procedures, include:

- The medical and financial sectors (especially banking), due to the high impact of privacy loss to the individual;
- Journalists, due to the importance to the public of a healthy and unfettered press;
- The public sector (government), due to the special duties owed to Canadians by the civil service and other government workers.

While "privacy" has never been defined in Canadian legislation, it is often considered the right to be left alone and the right to control one's own personal information. While "personal information" is defined in the *Privacy Act*, it often has a different meaning to the average Canadian. The *Privacy Act* does not consider personal information to include one's job title, telephone number or address, anything that might appear on your business card, or can be found through publicly available information such as the telephone book. Yet, many Canadians, when asked, consider *any* information about where they live to be personal.

Indeed, when surveyed, privacy appears to be highly important to Canadians. Surveys have shown Canadians focus especially on medical and financial privacy. On a recent Quebec television show, for example, viewers were urged to respond to the question "In the name of security, would you accept intrusion in you private life?" A stunning 85 percent of the 400 respondents answered that they would not accept such intrusions! While hardly a scientific study, it demonstrates the pulse of Canadians at this moment, who are perhaps beginning to feel dissatisfied with new intrusions that offer no guarantees of security.

Conversely, Canadians have often been extremely willing to give away their personal information or trade it for something negligible, such as the chance to win a prize. The attitudes of Canadians, therefore, do not tend to manifest themselves in corresponding behaviour.

It is unclear if Canadians merely pretend to be interested in privacy rights or if they simply do not grasp the connection between protecting their privacy and avoiding disclosure of personal information. It is important to note, however, that disclosing one's own personal information is consistent with privacy rights. If one has control over one's own personal information, he can choose to share it as he wishes.

Simplify Privacy for the People

The role of the Canadian people is often ignored when discussing the Canadian privacy environment, likely because so few Canadians are actively involved in protecting their own privacy rights.

One of the recognized failings with involving the general public in the so-called "privacy debate" is the failure to make the issues easy to understand and relevant to the individual. A related failing is the failure to make the necessary technology easy to implement and use. The lack of usability is a barrier to public engagement in matters of privacy. If, for example, P3P technology were to be embedded in Web browsers, people would use it by default.

The call for simplicity does not stop there. Laws, principles, directives and communications must all be easy to understand in order to be effective. Further, they also need to be meaningful to the consumer and continued on an on-going basis. In 1994, when Quebec passed *An Act Respecting the Protection of Personal Information in the Private Sector*, the province required companies to send consumers notices as to how their information would be used. It cost millions of dollars to Quebec-based businesses but the letters were inconsistent and confusing. Nine years later, even those consumers that understood the implica-

tions of the letters don't remember this information, and certainly don't know what policies are in practice.

Change the Way People Think

Some activists believe a better solution may be to focus on changing the behavior of Canadians in the long term. It must be recognized that Canadian attitudes and behaviours often require years or decades to develop. There are, however, many examples of public attitudes changing over time, resulting in a significant change in government and private sector policy. Lobbyists, for example, have demanded clear and complete food labeling for many years. Now Canadians expect all food labels to have detailed information and this information is strongly regulated by the federal government.

Perhaps, as happened for environmental concerns, it will simply take time for the public to understand the immense scope of the privacy problem within Canada. Schopenhauer famously said, "all truth passes through three stages. First, it is ridiculed. Second, it is violently opposed. Third, it is accepted as being self-evident." But in order for truth to pass through these stages, it must first be heard.

The Activist Community

The groups attempting to spread the word about privacy matters comprise the Canadian activist community. Privacy is a serious concern for activists in Canada. Despite a general public that is mostly uninformed, the privacy community in Canada is very informed and committed — yet rather scattered. Many of the Privacy Commissioners are considered part of the "privacy team" trying to educate the public, make privacy an important issue in the press, and have a meaningful impact on legislation.

This is important because the activist community in Canada is not well funded and has little infrastructure. In contract, activist organizations in the United States, such as the Electronic Privacy Information Center (EPIC) are extremely well funded and have enough power to speak directly to the government. More significantly, the government knows it is necessary to listen to the EPIC and other activist organizations because they are capable of energizing and galvanizing the public.

This sort of reaction is rarely seen in the public in this country due to the Canadian cultural resistance to speak out or drawing attention to oneself. Indeed, many of Canada's top privacy advocates are better known and appreciated in countries other than in Canada. This is not peculiar to matters of privacy or activism in general: it is a well-known Canadian quip that "to make it in Canada you have to *leave* Canada".

Fundamental Principles

Of all the sectors, activists are the only group that will promote the concept of fundamental principles of data collection. Even the activist organizations often get so involved with the details of negotiating a compromise to ensure some privacy principles are recognized, that they forget to express the fundamental principles. These principles are recognizing that any collection of information implies the risk that the information will be abused. The fundamental principle is that all collection of information is a breach of the right to privacy. If the debate starts with a question of compromise and balancing, then the fundamental principle is lost.

Who are the Activists?

Privacy activists may be university professors, computer professionals, business people, health professionals, union organizers, and directors of conservative "think tanks". Activist organizations are rarely devoted solely to privacy matters. Instead, they may be broad-based, such as the Public Interest Advocacy Center (PIAC) and various civil liberties organizations. Alternately, they may be focused on particular interests such as the rights of refugees, minorities, trade groups or freedom of the press.

The organizations and individuals that share an interest in privacy in Canada often have nothing else in common. Although there is no other common thread to unite these organizations, the common interest in privacy and the relatively small privacy community make it easy for Canadian privacy activists to share information. They do so through mailing lists, symposia, computer listservs and organized consultations in the development of legislation.

Meaningful Consultation

One of the challenges of the activist community is attempting to make an impact on the creation and design of legislation. The legislative process in Canada has specific standards and procedures. Depending on a number of factors, Canadian laws may take years to be enacted or may be rushed through into law in just a few months. The government is encouraged but not required to engage interested parties and to solicit their opinions about matters relevant to a proposed law before it is passed.

One example of this consultative process can be seen when Canadian members of Parliament attempted to push through legislation relating to Lawful Access. Unlike the usual consultative process, the government attempted to

push the law through in a very short time (and without any outside consultation). In response, activist organizations immediately demanded to be heard and their input considered. Quickly, three meetings were arranged and held across Canada to allow invited interested parties from non-governmental organizations, the press and the business community to voice their concerns and ask questions about the new legislation.

The response from the government is still pending but the activist community is wary about receiving a meaningful response. The Canadian government is known to fulfill the specific requirements outlined in its legal mandate without necessarily fulfilling the spirit. That is, the government will schedule meetings, attend them, take notes, file a report indicating what was said in the meetings — and then continue to implement the law, policy, measure or procedure regardless of the issues or concerns brought forward at the meetings.

This is not to imply that members of the civil service who comprise the government have a particular malicious intent or agenda in behaving in this manner. They simply have no incentive to do otherwise. Modifying the process requires extra work and there in no perceptible benefit in ensuring that meaningful consultation takes place (at least, from the point of view of the government officials). Further, civil servants will incur no penalties or sanctions if they fail to vigorously pursue the input of interested parties.

Rapid Enactment

At times, the government is adamant about dealing with a matter in a very short time, all options may appear to be untenable. Should one push to enact badly drawn legislation immediately so some effect is achieved, while leaving the law flexible enough for future amendment? The problem with this is the challenge of convincing Parliament to revisit a matter it sees as closed. Also, experience has shown that the more flexibility there is in a legal guarantee or definition, the less is firmly entrenched.

The alternative is to wait until one considers *all* opinions gathered over months of meaningful consultation, and then draw up an elegant law that has considered all sides. The problem with this is option is that the public may never engage in the matter, and it may be challenging to convince Parliament to revisit a situation they see as having been rejected by the very activists that are most concerned with it.

Many in the Canadian activist community are beginning to believe they often pay too much attention to legal means of legislating privacy. They are now expressing the intention to change their focus and work on modifying the overall message getting out to public. Many activists are choosing to focus on educating the general public and key influencers, rather than the monumental (and sometimes pointless) task of changing federal legislation.

Consequently, privacy commissioners routinely speak at law and business schools on this important matter. Others are attempting to reach the public even younger, by speaking at high schools. Still others are focusing on the press and media. Currently, their efforts are not well coordinated and the effectiveness of their efforts is variable.

The Government and Public Sector

Much is discussed in other parts of this document regarding the functions of the government and the legislative process. However, one point that should be recognized is that public law (as well as the entire regulatory system of Canada) allows a great deal of power to be discretionary. This affects the uniformity of application.

There is no champion of privacy issues in the Canadian Parliament, nor in provincial legislatures. Instead, the Privacy Commissioners bear the entire role of Canadian privacy champions and, as we have shown, often have no legal power to enforce privacy legislation.

As discussed in the following sections, new laws, measures and programs are being discussed and implemented in the aftermath of the September 11, 2001 terrorist attacks. Not surprisingly, the attacks were significant events affecting the development of privacy law and policy in Canada. Recognizing the compromising nature of Canadians, the Canadian government responded both to American demands for “increased security” and Canadian dissent in the matters of individual privacy. While certain anti-terrorist measures were hurriedly implemented, some debate did occur in the Canadian Parliament and several of the more draconian measures proposed by the Americans were actually rejected.

The influence of the United States on the Canadian legislative process cannot be ignored. Informally, American support is necessary to pass any Canadian privacy laws that may affect the United States. Since the United States is Canada’s major trading partner and seems to enjoy exerting its dominant position, it is often said that, “when America sneezes, Canadians catch a cold.”

Administering Privacy Protocols

Privacy protocols are not merely listed in the Privacy Act and PIPEDA. Instead, administration of personal information is

part of many Canadian laws, including those that regulate public bodies. The federal privacy commissioner's Annual Report lists several cases where personal information was retained, used and disclosed improperly, including:

- The Department of National Defense improperly retained information about pardoned convictions of an individual after the information was supposed to be expunged, and used that information to deny the individual employment opportunities. The Privacy Commissioner convinced the Department to reconsider the individual.

- Canada Post improperly disclosed information collected for its National Change of Address (NCOA) service. It engaged in negative consent by selling all personal information to mass-mailers unless individuals specifically requested their information be removed from the sold database. After much convincing Canada Post Agreed to changed its policy.

These cases may not appear to be particularly serious or heinous incidents. When civil servants are typically ignorant of the basic principles of privacy, however, and the basic requirements of the Privacy Act, it indicates a failure of the system to protect fundamental privacy rights of its citizens. Overall, several cases investigated by Privacy Commission showed that government bodies don't much consider the Privacy Act or basic principles of privacy as they go about their business.

Business and Industry

Like most people in Canada, those in the business and industry sector are often improperly informed about the fundamental principles of privacy. It is not their central focus, after all. They are interested in the specifics of their business. Privacy is generally considered a requirement that needs to be dealt with. It is seen in a similar manner as other regulatory matters that have no positive effect on sales, marketing or other money-making elements.

Indeed, if privacy is pursued within Canadian industry it is usually amalgamated with the concept of security. Privacy and security are so frequently grouped together that corporations often appoint a Chief Privacy Officer who also functions as a Chief Security Officer, with a dual mandate that emphasizes the security component.

When developing infrastucture technologies for the company, the corporate sector has been known to confuse privacy with security. It is security that is pursued as a means of protecting intellectual property, safeguarding clients and minimizing risk. There is a quantifiable business case for security. As a result, security has become recognized as a business necessity while privacy has largely been ignored by Canadian business.

In cases where chief privacy officers are effectively security officers, the problem of conflict of interest arises. Typically when privacy and security conflict in the business world, security wins out. Some of the typical privacy invasive activities that are generally accepted in Canadian businesses are:

- **e-mail monitoring** — In Canadian law, the owner of a particular electronic mail server may access any of its messages. This means that companies that provide e-mail addresses for their staff (without formally transferring property rights) are entitled to monitor all e-mail communications by staff members. When joining a large corporation, Canadian employees typically sign an employment agreement that says, in part, that the employer has the right to look at any e-mail the employee sends or receives through the corporate mail servers.

- **Telephone monitoring** — The same privacy intrusions apply for telephone communications. Many telephone lines are monitored in Canadian business, ostensibly to improve customer service and decrease possible litigation.

- **Video cameras in the workplace** — notice is required but most large workplaces are monitored for security. Banks, insurance companies, production lines and many other sectors are often filmed throughout the day.

Manufacturing Trust

While the September 11, 2001 terrorist attacks resulted in measures designed to increase government access to personal information, it has also spawned a backlash against corporate access to public information. Members of the public have become generally more distrustful and want to put their faith in the entity they believe they can trust – the Canadian government. Corporations, on the other hand, are considered more suspect due to their obvious bias of making money at (almost) all costs.

Consumers are frustrated with e-mail inboxes full of

spam sent by direct marketing companies. The public is increasingly more aware of identity theft and Canadian Internet users are becoming aware of the risks in offering personal information online. Although, this trend is extremely gradual, it may signify the beginning of a new direction toward increased privacy awareness among the general population in Canada.

In response, corporations are attempting to offer some assurances to the public that they are trustworthy. Corporate privacy policies have proven to be virtually useless. Most Canadian consumers do not read corporate privacy "guarantees" and proclamations. Those who do read these promises, believe they cannot trust them.

Web seals, also known as privacy marks or "trustmarks", have similarly failed to capture the confidence of the people. The initial versions had no objective standard and were voluntary. They also were poorly monitored and could offer no real guarantees over the life of the company, since corporate policies could change at any time with no legal remedies. The lack of consistency and comparability between different privacy seals and across jurisdictions also had a negative impact on public response. In the end, the absence of common, baseline international standards for privacy, data protection, auditing and compliance verification, mean that the growing proliferation of privacy marks and seals is likely to generate even more confusion on the part of consumers — and less trust.

The latest development in Web seals is the e-commerce seal that requires a specific standard to be met in dealing with financial information. So far e-commerce seals are voluntary and no widespread code has developed. It is too early to tell if these seals will be any more successful than their privacy counterparts.

Standards

The CSA Standard was developed by mostly corporate interests in response to the OECD's *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*. Since a policy had to be drawn up in order to ensure the European Commission did not impose trade barriers on Canadian companies, the Canadian business community decided to write the policy itself.

One major problem with the CSA Standard was that it was a voluntary code. The people involved in developing the standard hoped that a global standard for privacy could be developed, similar in nature to the ISO Standards, which are also voluntary. A major difference between these standards is that ISO Standards are based on specific objective criterion and procedures that can be followed uniformly. The purpose is to ensure that products are produced uniformly. Using ISO Standards helps to reduce lag time in production, helps the products get to market quicker, and helps to foster confidence by the public and investors. There is a demonstrable business case for ISO standards.

In contrast, privacy itself is notoriously difficult to measure because it has no baseline criteria. Experts disagree on the very definition and scope of privacy. Indeed, some consider it so abstract that it only has meaning in specific examples. Certainly, since privacy has different meanings and different values for different people, it is by nature not uniform. Some say that if privacy can't be objectively defined, it cannot be quantified. By extension, if privacy cannot quantified, it cannot be standardized, measured or demonstrated.

Privacy as a Business Case

Privacy commissioners and activists often say the best way to promote privacy in the public is to make a business case for privacy. If businesses consider it worthwhile to provide privacy for their customers, they will do so. Business, however, will only consider a measure "worthwhile" if it provides a clear financial gain — or avoids a clear financial loss.

To put it simply, businesses are interested in business. They want to avoid trade restrictions, lawsuits and government fines, so they are willing to implement some privacy protocols as necessary. Businesses also initiate measures when doing so generates a financial impact through positive public relations. In the United States, for example, businesses reacted quickly (and positively) to the Safe Harbor laws because those that did so were recognized admiringly in the press and media. Those companies that did not do so were vilified.

In Canada, the impact is somewhat muted. Canadians do not react as vehemently as do Americans to either positive or negative press. Further, there is little recognition of the dangers involved if privacy is breached so Canadians will not vilify those that do so.

Good privacy can be good public relations but, in Canada, the time is not yet right for business to put a significant value on offering privacy. The Canadian company Zero Knowledge failed in marketing many of its technologically advanced privacy products because it was ahead of its time. It seems consumers are not yet willing to pay for privacy. Businesses are unwilling to take the necessary steps, and pay the necessary costs, to ensure the privacy of their customers, simply because they see no financial return in offering it as a feature.

Simple and Uniform Laws

While businesses are willing to comply with privacy legislation if necessary or financially beneficial, they prefer a single, simple law to follow, as opposed to several different laws spanning various jurisdictions. As one government official stated, “the only thing companies hate more than having to comply with legislation is having to comply with multiple legislation.”

While provincial privacy laws must be “substantially similar” to *PIPEDA*, there are certain difference in administration, focus and procedure that makes compliance to privacy law difficult for companies that operate in more than one Canadian province or territory. This is further complicated by the fact that laws specific to a particular industry often have privacy elements enshrined, and it is not clear whether the privacy statute of the industry-specific law should have precedence.

This situation inevitably puts the privacy commissioner in conflict with particular industries. The Minister responsible for particular industries will inevitably side with his constituents for political reasons. This situation results in privacy measures being championed only by the Privacy Commissioner who, as we have noted, has no legal power to enforce compliance.

Specific Issues

This section looks in detail at specific issues that are most prevalent in the discussion of privacy in Canada.

Debating National Identification Cards

Since the September 11, 2001 terrorist attacks, several measures have been proposed as a means to increase security against terrorists through increased collection of personal information, tracking of movements and identification technologies. Though no clear explanations or empirical evidence have been offered to justify how these measures will make Canadians more secure, the debate continues and increased pressure is being brought by politicians to implement these measures.

A national identification card is one measure being promoted by the Minister of Citizenship and Immigration. It has been discussed several times over the past few decades but has never obtained the support of interest necessary to be initiated. In recent months, several stories concerning the issue have run in the press and media, but little appears to be decided.

As technology continues to develop, the possibility of implementing a highly personalized national identification card becomes more of a reality. In the past, it was difficult to overcome the threshold of work – to create a centralized national database, all the existing databases would have to be merged. The integrated nature of digital technology is constantly making this a less expensive and less work-intensive option. This may result in a backlash, however, if highly personal information such as DNA is included in the database. The Canadian public rarely reacts to infringements of its privacy but the collection of highly intimate personal information is more likely to cause a reaction.

Positive and negative sides exist for each issue:

Expedience versus Misuse

Centralization of data will be expedient because citizens will need only one card for identification for health insurance, driving, social programs and many other functions. The single database will save tax-payer dollars by eliminating duplication. In opposition, a single comprehensive file about all aspects of the life of an individual can be misused for personal, financial or political motives. As well, a centralized concentration of personal data about a large group is an inviting target to those who wish to perpetrate fraud or other illegal or immoral activity. Proscribing the use of the information except for particular purposes is ineffective unless perfect safeguards are built into the system to ensure the information cannot be accessed except for those purposes. Since the system must be operated and administered by people, it is impossible to have such a perfect system. Unauthorized, intrusive and unreported access to personal information is inevitable.

Diminishing Fraud versus the Devastating Effect of Errors

Biometric identifiers would make the card more accurate and diminish the likelihood of fraud. Social benefit and health care systems across Canada experience an extensive degree of fraud, including use of the system by ineligible individuals from other countries and multiple collection of benefits. In opposition, the problem with adopting technology as a solution is that it is imperfect and subject to human error, yet people consider it virtually infallible. There is no guarantee of accuracy in one central card, and the effect of an error would be more widespread since it would be linked to all elements where identification are necessary. In such a state, loss of a card could lead to loss of identity.

Greater Security versus Chilling Effect

The centralized collection of information by the state is often touted as a means to help secure the nation. There is no definitive proof of this claim, however some evidence shows that taking any measures may help calm public fears of insecurity, even if such measures are ineffectual. In opposition, collecting personal information in a giant database available to various branches of government offends the basic principles of privacy. These are that personal information should be used only for the purpose for which it was collected, and that individuals should be able to decide for themselves how the information will be used. Use of a national identification card brings to mind totalitarian regimes where law-abiding citizens can be stopped at any time and asked for their papers. It transforms the citizen's relationship with the state.

No Public Opinion

It must be recognized that the Canadian public has not expressed itself significantly either positively or negatively in regards to the prospect of a national identification card. Few understand the implications, and fewer still bother to make their opinions known. There is a general desire for greater security since the September 11 attacks but this desire is vague and unfocussed.

Existing Identifying Documents

Canada already has certain legislated identification cards. Each province administers it's own public health insurance, and anyone who wishes to obtain health care must first present their own personal health card. Most include a facial image and must be periodically renewed, but previously obtained permanent cards with no image remain valid in some jurisdictions. Other identifying documents include passports, driver's licenses, and other use-specific licenses including for gun registration and fishing permits. Canadians also use plus several private cards including credit cards, store-specific cards such as movie rental cards and frequent shopper cards, and third party loyalty cards such as AirMiles®.

The most common unique personal identifier used at present in Canada, Social Insurance Number ("SIN"). The number is required on many different types of documents, including employment agreements, financial records, mortgage documents, tax returns, social program applications and more, under the specific legislation listed in the Resource Guide. The card bearing the number is rarely required, except as a memory aid. Citizens must apply for the number in order to legally engage in these activities and the application is generally administered in schools, for the sake of expediency, presuming that everyone will wish to be employed, for example. Without properly educating youths about effects and usages of the SIN, the effect is to compel citizens to obtain an identification card.

The SIN was established in 1964, replacing the national unemployment insurance number and adding functionality to administer the government's Canada Pension Plan. At that time, the then Canadian Prime Minister assured his country that the SIN would only be used to administer unemployment insurance and the newly implemented Canada Pension Plan and no other use was anticipated or permitted.

In recent years, the SIN has been requested by increasingly more commercial enterprises. While they have no legal right to demand individual Canadians supply their SIN numbers, they are also not precluded from requesting it as a simply identifier. Most people in the general public are unaware of their rights and any dangers in providing more personal information than is necessary. Most people will let clerks or shop-keepers view their SIN, driver's license or other identification documents if it is requested for any reason.

Function Creep

So-called "function creep" is a recognized problem with the SIN and would presumably be a problem with any national identification card. It refers to the situation where laws or tools are created for one specific purpose and gradually become used other purposes, while the safeguards built into them and important to the designers are amended away. This is especially prevalent when considering the collection of information. The Social Insurance Number was created to administer pensions and employment insurance, but three years later the (now-named) Canada Customs and Revenue Agency began using it for tax collection purposes. Today is used in hundreds of different transactions and kept in almost all governmental databases, and many private and commercial databases.

There is a general belief among privacy advocates that the SIN is insecure, and significant anecdotal material to support this claim. There have been incidents of identity theft and fraud relating to SIN abuses, along with denial of benefits relating to SIN errors. Surprisingly, there has not been a comprehensive study or survey conducted to identify systemic problems with the SIN. Prior to expanding the idea of a national identification card, it would be advisable to recognize what problems have developed using the existing system.

Another argument used to support a national identification card is that the SIN is effectively being used as a national identification card, so it should be recognized as such and incorporate all the accuracy benefits new technology can offer. This argument legitimizes function creep as a benefit instead of a problem.

Considerations

It is likely that the implementation of a national identification card will continue to be debated. In any such debate, it is important to consider the following issues:

- How will privacy be protected, abuse be avoided, and improper access denied?
- How will technological changes affect the use and linkages of data?
- Will a national identification card be fiscally responsible, saving taxpayer dollars through minimization of duplication?
- Do citizens want the expediency of a national card, even if it means giving up significant privacy protections and risking identity theft?

Cross Border Travel

Accessing Airline Passenger Information

In late 2001, under amendments to the *Customs Act*, Customs officers were given access to Advance Passenger Information (API) and the detailed Passenger Name Record (PNR) about every passenger flying into Canada from a foreign destination, including Canadian citizens. The stated intention of these amendments was to attempt to identify criminals by their travel patterns. The Canada Customs and Revenue Agency ("CCRA"), the administrative body for Canada Customs, undertook to destroy all provided information within 24 hours unless information warranted secondary screening. In summer 2002, CCRA decided to keep all information for six years in a massive database, dubbed the "Big Brother" database. This information will be available to all government branches under information-sharing provisions of the *Customs Act*.

This represents not only a recent example of function creep, but also a massive change to the way the personal information of law-abiding citizens is treated within Canada. Privacy commissioners across Canada, along with the activist community have universally condemned this measure as an unwarranted invasion on the privacy of individuals. The federal Privacy Commissioner stated "Government has no right to create a massive database of personal information on all law-abiding citizens for no other purpose than to use against us if it becomes expedient." His request to limit its use to identifying terrorists has been flatly refused, so the database can be used to search for individuals suspected of illegal money movements, tax evasion, and those wanted on outstanding warrants.

While many would consider this ability to identify regular criminals to be a benefit, there are serious privacy concerns to weigh against this benefit. Individuals will not simply be identified by their names and compared against a database of outstanding warrants. The patterns of behaviour of all airline travelers would be rigourously analyzed, including methods of payment, dietary requests, and even neighbouring passengers. If a recognized criminal happens to be assigned a neighbouring seat, this information will be retained in an individual's file. The potential to use such information to target an innocent individual is clear.

Balancing Privacy with Criminal Investigation

Similarly, the new *Public Safety Act* of 2002 (Bill C-17) includes a provision that gives federal law enforcement agencies — the RCMP and CSIS — the right to use airline passenger information to conduct anti-terrorist screenings. While many might consider this a reasonable limit to privacy under the Charter when weighed against possible terrorist threats, the concern is the likely use of this information to screen for any and all criminal offenders. The Act refers to persons wanted on "warrants" as opposed to persons wanted for suspected terrorist activities.

This broad wording has been justified to ensure suspected terrorists cannot escape apprehension on a technicality. This is a reasonable concern, recognizing the perceived imperative to fight terrorist threats and the balancing of rights against the public safety. However, the broad wording also makes it likely that all police will use the information to investigate any *Criminal Code* offences. Police have a duty to investigate crime using any means legally available to them. If the information is available, they will use it. Unless use of the information is specifically limited to identifying terrorists it will be used against all others wanted on warrants.

Again, the privacy concerns must be weighed against the potential benefit. Canada has a long-established system of law enforcement investigation procedures. There is a general right to anonymity under Canadian law — individuals are only required to identify themselves to police when being arrested or carrying out a licensed activity such as driving. Neither category fits when boarding an airplane but the airline has a legitimate transactional right to require identification in this case. If this information is automatically shared with law enforcement, it creates a new compulsory requirement to self-identify to police. Further, it makes the airline an agent of the state in law enforcement — something that is not allowed under the Criminal Code.

Without access to this information under the Public Safety Act, a police officer would need to show probable cause to obtain a warrant issued by a judge. The officer would need to identify a specific crime under investigation and show that there is a substantial reason to believe the information contains evidence relating to that crime. With the information, the officer can search through personal information not otherwise available to him in the hopes that it will produce information relating to a crime. This "fishing expedition" is not permitted under Canadian law except under extreme cases, such as responding to a terrorist threat.

Non-universal Application of Law

A minor point is the non-universal application of the law. If such measures are considered beneficial and they assist in identifying terrorists, why are they limited to international air travel? Why not use the information access measures at all borders, or for internal Canadian travel? Why limit the information gathering to travel? The obvious

explanation is that these measures were designed in response to the September 11 terrorist attacks, so the public is more likely to accept intrusive measures without question when they involve international air travel. However, CCRA has announced its intention to expand the database to include all forms of cross-border travel.

Experts studying terrorist activity, database analysis and identification technology have indicated that there is no evidence that collecting such information will assist in identifying terrorists. Thus the test for expediency is not met.

Meanwhile Canada and the United States agreed as of December 2002 to share information on "high-risk travelers" entering either country. In September 2002, initial projects were established to test the possibility of using joint customs and immigration officers.

Sending Personal Information Across the Border

Banks in Canada are heavily regulated only five major national banks exist, although there are also smaller credit unions, caisses populaires and other financial institutions. The Royal Bank, the largest of the five major national banks, recently became a part owner of Regulatory Datacorp and pledged to become a customer.

In doing so, it will share identifying information about its customers with an international conglomerate that cross-checks the names of these customers against the large Global Regulatory Information Database (GRID), containing the names of "suspicious" individual including criminals and money launderers, along with journalists and close relatives of political figures. If your name is on the GRID, your file will be flagged for further investigation and scrutiny, and a report will be sent to the bank.

The stated purposes of the company are to combat banking fraud, money laundering, and other crimes, as well as to watch for suspicious activities that may be undertaken by terrorists or drug cartels. At the corporate headquarters in the United States, such investigation of customers by financial institutions is permitted and may even be required by the *U.S.A. Patriot Act*. Canada has not demanded such activities of its banks. *PIPEDA* super-cedes the Bank Act in the administration of personal information by Canadian banks, so banks are subject to the same duties and responsibilities as all other corporate entities.

Concerns include the likelihood of errors and system flaws leading to serious discrimination. Mistakes in data entry or having a common name or a name similar to a known criminal could result in a customer's file being flagged. It could impact on a customer's credit worldwide, resulting the customer being unable to obtain basic services such as mortgages, loans and insurance. Depending on the eventual expanded use of the database by parties other than financial institutions, it could also result in harassment or denial of entry into other countries, and improper arrests. All this is possible without the individual having any knowledge of or access to his file.

Privacy Impact Assessments

The Privacy Act requires government agencies and departments to conduct Privacy Impact Assessments ("PIAs") on any new technology, program or initiative before it receives funding to implement it. PIAs are reports of studies of the privacy implications of a particular project, including risks, types of infringements that are likely to occur, and how such risks and infringements can be minimized.

Guidelines to conduct these PIAs are available and timelines are specified by the Act. The four core components of a PIA required under the Privacy Act are:

- project initiation in which initial privacy related concerns are considered;
- data flow analysis which looks at the project's proposed business processes, architecture and the flow of personal information;
- privacy analysis which examines the data flows in terms of applicable privacy legislation and policies;
- privacy impact analysis report which evaluates the privacy risks and the implications of those risks.

PIAs in the Canadian Context

The problem is that the legislation requires nothing more than the completion of a PIA. This means agencies must assess the state of privacy in their departments but need not correct any problems, and there is no provision to deny funding to projects that are privacy invasive. Further, since the PIAs must be completed *before* the project is implemented, the assessment can only be conducted on the proposed measure, which is likely to be modified somewhat during implementation. There is no requirement for further assessment or periodic review, and no system of audit or oversight. The report is sent to the Privacy Commissioner and the results of these PIAs are also supposed to be summarized and made available to the public, however this requirement is frequently ignored. There is little penalty for failing to provide such a summary, and the related government agencies have no interest in enforcing the requirement.

This is an excellent example of an attempt to initiate

an important privacy measure that has failed because it was badly conceived. As a result, government bodies pay little attention to the PIA, merely fulfilling the minimal requirements in order to obtain funding.

Dangers of Improper PIA Implementation

The dangers of such a policy are that privacy risks will be considered irrelevant to design considerations, and that privacy risks will be ignored once they are written into the completed document as one task checked off the list, thus they will not be corrected. The function of a PIA is to be a working document, constantly updated as design changes occur, used to recognize and minimize the privacy risks inherent in any project.

The lack of proper reporting and enforcement is another problem. The Privacy Commissioner receives the PIA but has no authority to require changes that would better reflect the principle of protection of privacy. Without an available summary, the public is left uninformed of potentially serious privacy risks. Finally, the basic thinking behind the PIA is ignored if it not shared with all the interested parties designing and implementing the project.

Creating a Privacy Framework

A PIA will maximum effect if it is used as part of an overall privacy framework involving legislation, policy and technology.

Legislation can be used to require standard elements, being:

- Commitment to best privacy practices;
- Development of the PIA in conjunction with the development of the project;
- Periodic reporting to all parties involved in development or review of the project;
- Review, audit and oversight of the PIA;
- Enforcement of the measures outlined in the PIA.

Policy can be used to determine priorities when weighing the various goals of the project against privacy risks. Certain projects must be undertaken despite the privacy risks, depending on the goals and needs of the government.

Technology can be used to minimize the privacy risks while upholding the project goals. Indeed, it is imperative to combine these components so that privacy can be built into the design of the project. Privacy enhancing technologies (PETs) can be integrated into the initial design and new elements are likely to be considered in response to problems, flaws or opportunities discovered during the implementation process.

Measuring Privacy

Peter Hope-Tindall, a recognized Canadian expert on PIAs, suggests using a three-dimensional privacy metric to measure the success of a privacy solution. The three elements are:

- **Identity** — how much is the information personally identifiable, ranging from being completely anonymous to being completely identifiable;
- **Linkability** — how much data is linked to other data, recognizing that individuals can be profiled using the combination of minimally identifying information if sufficient information is collected;
- **Observability** — how easily can individuals be identified and how many links can be developed by using the system in the way it was designed to be used.

Data minimization is always a goal of PIAs. Creating a privacy framework, however, can have the added benefit of making the entire project more effective. The framework is an excellent design model for minimizing data flow. Less data flow generally means greater efficiency, as less information must be collected and processed.

PIAs were required for the new anti-terrorism legislation initiated after the September 11 terrorist attacks. Unfortunately, without the requirement to ensure privacy risks are minimized or conduct any sort of review, audit or post-implementation follow-up, these PIAs would have had no effect on the development of highly intrusive measures. Had the PIAs been conducted in the manner suggested above, it is likely that the resulting measures would have been more effective and less privacy intrusive.

International Obligations

Canada is a sovereign country but international events and pressures constantly and consistently impact upon it. As mentioned earlier, Canada is subject to the OECD fair information practices outlined in its *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*. Canadian commercial interests developed the CSA Model Code in response to potential trade barriers that might have arisen out of the requirements of the 1995 *European Union Privacy Directive*. This code was eventually made into PIPEDA and passed as legislation when it became clear that a voluntary code was not sufficient for the European Union. The EU only agreed that Canada complied with the Directive in January 2002, after review-

ing the implementation of the new law.

Since 2000, there has been increasing pressure toward implementing national security measures that are privacy invasive. These were initially sparked at the passage of the Council of Europe's Convention on *Cybercrime* in 2000. (The lawful access provisions relating to Canada's signing of this Convention are discussed in more detail earlier in this report.) The attitude galvanized following the September 11, 2001 terrorist attacks.

US Influence

Canada feels particular influence from the United States (US) due its proximity, cultural similarities, and overwhelming trade power. The US is Canada's largest trading partner and, with Mexico, comprises the North American Free Trade Region. Canada and the US also share the world's longest undefended border. Canada is also virtually dependant upon the United States for defense against hostile attact, however it is generally recognized that there would be little likelihood that Canada would be attacked for various reasons:

- It represents a "buffer zone" for the United States between Russia, so extensive US bases have been developed in the far north region of Canada;
- The location of Canada makes it geographically distant from anywhere except the United States and Russia;
- The huge size of the country would make it difficult to manage if attacked and conquered by a foreign power;
- There is little to be gained by attacking Canada as much of the country's value is in its intellectual property and its natural resources that take time and effort to exploit. In other words, there is little material wealth to immediately plunder;
- Canada is not seen as a hostile nation so it generates little hatred.

Still, the influence and pressure wielded by the United States — both government and industry players — cannot be ignored. Most political theorists and critics in Canada believe that no major policy can be passed without the implicit or explicit approval of the American interests.

Information Sharing

Since September 11, 2001, Canada and the United States have undertaken discussions relating to the widespread sharing of personal information, especially relating to immigration and border-crossing. Broad-based US/Canada joint "smart border initiatives" are being proposed and developed by private and public sector implementers. The benefit for Canadians is increased ease of crossing the US border, which has become more difficult, time-consuming and, in many reported cases, personally invasive over the past few years, and especially since September 11. 2001.

The negative side of this enhanced integration is the increased databasing and sharing of personal information as well as an almost paternalistic view by the government that privacy intrusions are "in the public's best interest."

The initiatives include information sharing on "high-risk travelers"; the development of common standards for biomentrics to be used on identification; the development of parallel immigration databases to facilitate easier and more regular information exchange; joint customs and immigration screenings and analysis; visa coordination; pre-clearance for air travel; and several other specific points aimed at harmonizing information relating to air, water and land travel. This information will relate to both personal and commercial border crossings.

Particular focus is on law enforcement activities. With the development of a Memorandum of Cooperation, the Canadian Royal Canadian Mounted Police (RCMP) and the American Federal Bureau of Investigation (FBI) will implement an electronic system for the exchange of criminal records information, including fingerprints, using a standard communication interface.

Passenger Database

The most significant development is the Advance Passenger Information and Passenger Name Records (API/PNR) on high-risk travelers destined to either country. Canada implemented its Passenger Information system (PAXIS) at Canadian airports on October 8, 2002, to collect Advance Passenger Information. The automated US/Canada API/PNR data-sharing program is scheduled to be in place by Spring 2003. We discuss the issues relating to this airline passenger database earlier in this report, but important elements of this database and the related initiatives are:

- It is classified so Canadian citizens will have no way to know what is contained on their file or even if a file on them exists. There will be no opportunity, therefore, to rectify errors.

- There is no clear indication of what criteria will be used to identify a "risk to transportation security" so

travelers may find themselves pulled aside and interrogated due to their involvement in lawful activities such as political protest. Considering that Canadians are routinely photographed by American intelligence officers when lawfully protesting at the American embassy in Ottawa and at American consulates throughout Canada, increased use of face-identification software poses an especially pernicious threat to freedom of speech and democracy.

- Since the information would be shared between countries, Canadian laws would be irrelevant regarding the safeguarding of information that has passed to the US.

Tracking Financial Information

Prior to September 11, 2001, the main focus of transborder issues was money laundering. In 1999, it was estimated that between $5 and $17 billion was illegally moved through Canada annually. At the G-8 Summits, there has been much discussion about coordination on tracking money from drug cartels and organized crime syndicates. In Canada, the *Proceeds of Crime (Money Laundering) Act* came into force on June 14, 2001. It gave law enforcement agencies broad powers to seize documents where there are reasonable grounds to believe offences relating to money laundering or terrorist financing are being committed. It also requires the reporting of suspicious financial transactions and of cross-border movements of currency and monetary instruments.

The Act was renamed the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and various provisions were added in December 2001. One of the amended purposes is "to assist in fulfilling Canada's international commitments to participate in the fight against transnational crime, particularly money laundering and the fight against terrorist activities."

Medical Privacy

Medical privacy is considered a special area of interest to those concerned with privacy because of the intimate nature of the information that might be collected, used and disclosed. The Canadian Medical Association (CMA) has outlined a voluntary *Health Information Privacy Code* that its members are supposed to follow. The CMA Code was based on the Canadian Standards Association's *Model Code for the Protection of Personal Information* (the "CSA Code"), and limits collection, use and disclosure in a similar manner. The problem, as with any voluntary code, is in ensuring compliance.

On January 1, 2002 *PIPEDA* went into effect for health information. The one-year delay afforded this sector was due to lobbying by powerful interests. Still, matters of public health and medicine are under the jurisdiction of the provinces and not the federal government. So far, only Albert, Manitoba and Saskatchewan (the so-called "Prairie" provinces of Canada) have passed legislation specifically dealing with health and medical privacy.

Socialized Health Care System

Every citizen in Canada is guaranteed the right to universal, free medical attention and care. Each province operates a socialized health insurance program for which registered users are given an identification card. The various systems are centralized within their own province and doctors and medical facilities bill the system directly for medical procedures and services.

Unfortunately, fraud is rampant in these systems. Medical fraud occurs on two levels — doctors making fraudulent billings and individuals using services for which they are not entitled. There are challenges in protecting privacy while auditing and investigating fraud in both circumstances. The challenge is greater when investigating fraud by the medical practitioner because doing so necessitates opening the files of his patients.

Provinces have responded to fraud in using services by initiating projects to increase the reliability of the cards. Biometrics have been installed in many cards, such as facial photographs. However most jurisdictions have allowed "grandfathering" of the previously distributed cards — meaning people who have cards without the additional security measures can still use them for the remainder of the period for which it is valid (in some case, for the rest of their lives). The new cards generally require periodic renewal as another security measure.

Where is Information At Risk?

Paper-based and electronic patient records, hospital and laboratory records, and the use of genetic-test information are among the most obvious areas where privacy protocols are needed.

It is easy to recognize the lack of attention to privacy matters when visiting any hospital in Canada. Frequently, computers containing hospital-wide patient databases are left on and unattended, even in remote corners of the hospital where no staff members are nearby. File encryption is rarely used and, when it is part of the procedure, passwords are often pasted to computers on yellow sticky notes.

Paper-based patient files are often left in open containers outside examination rooms, and are easy to access by anyone passing by.

Medical data has leaked to the press concerning well-known individuals including Toronto Maple Leafs hockey coach Pat Quinn and former Canadian Prime Minister Brian Mulroney. It is only in these high profile cases that the public is made aware of the extent to which their medical information is at risk. The majority of Canadians, however, still retain their false sense of privacy since they conclude they are too insignificant to warrant any attention.

In private medical practices, files of several patients are often left in the examination room while a particular patient is left alone to change clothing. These files contain identifying information (such as the patient's name) along with the detailed history of the patient including the doctor's own comments. Interestingly, doctors often attempt to deny patients access to their own files because of the personal opinions that may have been expressed by the doctor or other doctors that had been consulted, yet the information is often available to them if they care to sneak a look.

Poorly Designed System

At times, the problem is not the failure of the health care providers and their staff to fulfill basic privacy protocols. The problem may be systemic. The Ontario Information and Privacy Commissioner was recently involved in a situation in which one man's information remained incorrect despite the fact the database administrator had been made aware of the error. The failure to correct the error was not malicious. Rather, it was part of the bureaucracy. The commissioner found that the system was not designed to allow for the correction of incorrect information.

The system was, however, sufficiently open to allow the man to obtain a list of all charges billed to his provincial health insurance agency ("OHIP") account by a particular doctor. After discovering many falsely listed charges for treatments that were never received, the man reported the incorrect information to the Ministry of Health. The doctor was convicted of fraud for the false charges and the man asked for the incorrect information to be removed from his record. Many of the entries could prove extremely embarrassing and may affect his ability to obtain employment, insurance and other basic elements of life if the information was viewed by others, especially insurance companies or future employers.

It should be noted that insurers routinely require access to detailed medical records before providing insurance. This is not considered a breach of medical privacy as it is a contractual matter – the insured party is not required to authorize such access but the insurer is not obligated to offer coverage without it. Of course, this brings up another problem with the system. If all insurers routinely require such access (and they do) then individuals are effectively being denied the ability to obtain insurance unless they give up their right to privacy.

The Ontario Ministry of Health refused to delete the inaccurate claims, stating that the records showed transactional information that had been paid out. They stated that they needed to retain the information for audit purposes. The man was permitted to add his own statement of disagreement disputing the claims, but the Ministry would add no official record of the fraud conviction or the recognition that the services listed had never been requested or performed.

The Commissioner was able to intercede on behalf of the man, and extended this intercession to include the other patients of the particular doctor. The problem of a poorly designed database with no provision for error-correction remained. A further problem demonstrated by this case is the unwillingness of officials to take reasonable steps to assist individuals when it is obvious a design-flaw has put privacy at risk. Indeed, even when the Commissioner interceded, the Ministry decided not to participate in mediation but required more formal, adjudication of the matter. Finally, it should be recognized that the doctor's fraudulent activity was only discovered because the patient was proactive in requesting his file. A better audit system would have made it less likely that the doctor could engage in such activity.

Jurisdiction and New Legislation

In this instance, the Commissioner only had authority to act in this case because OHIP fell under the jurisdiction of the provincial *Freedom of Information and Protection of Privacy Act* (FIPPA). Most health care providers in Ontario, however, do not come under this legislation so the Commissioner has campaigned to pressure the Ontario government to introduce extensive personal health privacy legislation.

Despite proposals for a new, more stringent law called the *Privacy of Personal Information Act*, comprehensive privacy protection legislation covering the commercial, not-for-profit and health sectors, the legislation was never passed by the provincial legislature. The Act would have introduced far-reaching measures for ensuring patient privacy including the use of biometrics and PKI in smart cards for the electronic patient system. At present,

only three Canadian provinces have specific health-related legislation, and the federal equivalent takes effect in January 2004.

The Report of the Commission on the Future of Health Care in Canada

In April 2001, the federal government established a commission to investigate and report on the future of health care in Canada. The report is known as the "Romanow Report" after the commission chairman Roy Romanow. This report was released on November 28, 2002 and the response from privacy advocates has been overwhelmingly negative.

It includes the proposal for a Canada-wide electronic health record, but it is vague about who all will have access to the information and how previously identified privacy risks will be cured. In fact, the report proposes that a three-party team of specific government established and funded organizations would jointly administer the system. None of these organizations is authorized to provide health care to Canadians, so it is reasonable to assume that there will be at least three partially private organizations that will have full access to the medical records of every Canadian. This is contrary to the non-specific guarantees offered in the report that Canadian privacy would be protected. It is possible that other safeguards will be built into the system, but none is outlined in the report.

Law Enforcement and Surveillance

Canada's law enforcement agencies are divided into:

- The Royal Canadian Mounted Police (RCMP) — Canada's national police force
- Various provincial police forces in certain provinces (Ontario has such a police force while British Columbia does not, for example). Where a provincial police is not installed, the RCMP takes its place.
- Various municipal police forces in the major cities in Canada (including Toronto, Ottawa, Montreal and Vancouver). Some smaller cities and major regions in the under-populated far north of the country are also served by the RCMP.

As well, there are two other agencies that have no powers to arrest (and hence are not defined as law enforcement agencies) but have extensive powers of investigation:

- **Canadian Security Intelligence Service (CSIS)** — considered the Canadian "spy" agency. CSIS is roughly analogous to the intelligence portion of the American FBI (although the FBI also functions as a domestic police force for more serious crime as well as crimes that cross state boundaries).
- **Department of National Defence (DND)** — this department is responsible for the national security of Canadians, and administers Canada's Signals Intelligence (SIGINT) organization known as the Communications Security Establishment (CSE). The Communications Security Establishment is roughly equivalent to the American National Security Agency (NSA) and Defense Security Agency (DSA) or Britain's GCHQ.
- Unlike the Americans, the British, the French and other countries, however, Canada does not keep an intelligence agency that operates outside its own borders such as the American Central Intelligence Agency (CIA) or British Military Intelligence Group 6 (commonly referred to as "MI6" but known officially as the Security Service).

Each policing authority is required to abide by the Canadian *Criminal Code* and the Constitution including the *Charter*. Each is required to pursue the investigation and prosecution of criminals to the best of its ability *within the law*. There is a general requirement in the Privacy Act to collect only the minimal amount of personal information required for the intended purpose, and only to do so when there is a demonstrable reason for the collection. Usually, in order to obtain personal information, law enforcement personnel must get a court order, or warrant.

There is frequently a conflict between law enforcement and privacy advocates. Law enforcement agencies claim that greater access to personal information would make it easier for them to do their jobs of catching criminals. Privacy advocates warn that such access is contrary to privacy rights of law abiding citizens and may lead to abuses by individual members of law enforcement agencies or by others who manage to obtain such access through legal or other means. This conflict is not particular to Canada.

Canada's Spy Agency

CSIS was established in 1984 in response to perceived failures by the RCMP to effectively collect, analyze and retain information concerning threats to the security of Canada. Despite the fact that many CSIS officers were originally from the RCMP, the two services don't usually share information and have been described by insiders as having "icy"

relations with each other.

CSIS has wide powers to access personal information, including hospital files, income-tax returns, passport information, employment insurance, welfare records, memberships and associations. As a limitation of this access power, CSIS agents must obtain a warrant from a Federal Court Judge before access is granted.

The agency reports directly to specific government offices regarding perceived risks. Its role in investigating matters of national security affords it some exceptional privacy measures. Both the *Privacy Act* and the *Access to Information Act* have specific exceptions limiting or denying the public access to records relating to current or past CSIS investigations.

There is an oversight and review body for CSIS, known as the Security Intelligence Review Committee (SIRC). In addition to overseeing the actions of CSIS agents, the SIRC also reviews reports of the Director of CSIS and directions issued by the Minister of Defence. Finally, the SIRC responds to complaints made by citizens regarding the conduct of the Service.

Employing an estimated 2000 individuals, CSIS is one of Canada's largest government departments. Its estimated annual budget of $157 million in 2000 was sharply increased by 32 percent in December 2001 to help the Service respond to the increased terrorist threat brought on by the September 11, 2001 attacks on America.

Communications Security Establishment (CSE)

The Communications Security Establishment (CSE) is a civilian agency of the Department of National Defence. There is little authoritatively known about the activities of CSE and DND as these are classified for purposes of national defence. As was noted earlier, the CSE is roughly equivalent to the American National Security Agency (NSA) and the Defense Security Agency (DSA) or Britain's GCHQ.

CSE processes signal intelligence or "SIGINT", defined as "all processes involved in, and information and technical material derived from, the interception and study of foreign communications and non-communications electromagnetic emissions." CSE then analyses the information and reports to DND and other agencies. Collection of SIGINT is conducted by the Canadian Forces Information Operations Group (CFIOG), formerly known as the Supplementary Radio System (SRS), a component of the Canadian Armed Forces that operates under the direction of CSE.

There was no oversight body for CSE prior to 1996. At that time, the Defence Minister appointed the first Commissioner of the Communications Security Establishment. The Commissioner is given full access to all records and documentation on the CSE in order to write an annual report submitted to the Defence Minister, which is then reported to Parliament. No public disclosure of information is made about this agency and most Canadians don't even know of its existence.

It is unclear if CSE monitors Canadian citizens, either within Canada or abroad, despite the assurances that its mandate restricts it to monitoring foreign communications. It is well known that CSE works together with other security agencies in countries such as the US, UK, Australia and New Zealand. Despite denials, it is also well known that this combined security force operates the ECHELON surveillance system that routinely spies on individuals worldwide using privacy invasive technology.

Video Surveillance in Canadian Streets

There is no widespread use of closed circuit television (CCTV) for video surveillance by law enforcement agencies in public places in Canada. One of the main reasons the Privacy Commissioner publicly rejected its use in Canada is that it has proven useless in the United Kingdom against its stated goals of fighting terrorism, and meanwhile the statistics of violent crime have increased. People often forget that paying for more videocameras means there is less police budget available for police officers, so fewer crimes can be stopped as they happen (or prevented by a visible police presence). Besides, the evidence of the United Kingdom shows that if there is any effect on crime it is merely to displace it to another part of town where there are no videocameras, or to encourage criminals to hide their faces.

A few years ago, the RCMP installed video cameras in the town of Kelowna, British Columbia, an area under its jurisdiction. The stated aim was to prevent or deter crime. In response to the Privacy Commissioner's concern, the RCMP agreed to cease constant videotaping and only record when a when a violation of the law is detected. This response appears ludicrous as there is no way to determine when a violation of the law is occurring unless one is already a witness to it, in which case there is no purpose in having a videocamera at all. Besides, there is no assurance available to guarantee the taping would not take place continuously. As discussed elsewhere in this report, the Privacy Commissioner has brought a challenge in the Federal Court on this matter.

In another instance, a private security company installed videocameras in the main street of Yellowknife,

Northwest Territories. The purpose was to promote the services of the company. Being a commercial activity, *PIPEDA* applied and the collected images of individuals were considered personal information. That meant the company would have been required to obtain consent from all individuals being taped before the videotaping could occur.

Informed Consent and Warrants

The question of what is meaningful consent remains an issue. CCTV is used in the workplace and in other private locations where the public has access, such as banks, shopping malls and parking lots. Employees generally agree to such surveillance as part of their employment agreement, and consumers are warned that they may be videotaped in signs placed about the physical location. Specific limitations are enumerated in consumer protection laws prohibiting, for example, videotaping consumers in changing rooms of department stores.

The Manitoba Taxicab Act added regulations effective July 1, 2002 to require the installation of security cameras in all taxicabs. The stated purpose was to protect the safety of drivers. While the information and privacy commissioner of Manitoba has not objected to the use of cameras in this case, the Ombudsman's office has announced a review to ensure the information will be collected, used, disclosed, retained and disposed of in a manner consistent with Manitoba's *Freedom of Information and Protection of Privacy Act.*

Following a criminal incident, the footage from such locations is routinely shared with police on a voluntary basis. If the owner of the footage is not willing to hand over the tape voluntarily, it is relatively simple to convince a judge of its usefulness in an investigation and obtain a warrant to compel the tape be produced.

Intercepting Private Communications

It is an offense under the Criminal Code to intercept private communications, except under a court order. This means private individuals have no right to do so. There are, however, contractual options under Canadian common law available to overcome this apparent limitation. Employers that provide an e-mail address for the use of their employees have the right to monitor the communications using that address because it is considered the property of the employer. Increasingly, employers also monitor Web traffic on the computers of employees, ostensibly to prevent (or, at least, warn) if employees are visiting sites inconsistent with work-related Internet surfing. Such uses might include visiting pornographic or gambling sites, and commercial software is currently available to clandestinely monitor all Web traffic at organizations.

Generally, employers are expected to give notice to the employees that such monitoring may be done and various privacy commissioners have been involved in cases where insufficient notice is provided. Similarly, employers would have the same rights to monitor telephone conversations of employees when conducted on office lines.

Several laws regulate the use of information provided by customers. These include federal laws such as the *Telecommunications Act*, the *Bank Act*, the *Insurance Companies Act* and many others. Provincial and municipal laws also guarantee basic rights to consumers in particular sectors such as health and pensions.

Use of Technology Constitutes Search

Police are increasingly using new technologies for investigations and prosecutions, and it is up to the courts to interpret the implications of using these new technologies. The Ontario Court of Appeal ruled that police must obtain a warrant before using infrared aerial cameras during investigations because use of such technology constituted a search, despite the fact that police had not physically entered the premises.

These Forward Looking Infra-Red (FLIR) aerial cameras are widely used by law enforcement agencies across North America. The cameras can detect internal heat patterns and they are used in marijuana investigations because the lights used in grow operations give off an unusual amount of heat. Charter privacy protections were cited as the reasoning behind the decision, recognizing that "FLIR technology discloses more information about what goes on inside a house than is detectable by normal observation or surveillance."

Lawful Access to Communications

Generally, for police to obtain a court order to intercept private communications there must be sufficient grounds to obtain a warrant and the officer must establish that "other investigative procedures are unlikely to succeed". It must be more than simply the most efficient manner to obtain the information; it must the only reasonable means of obtaining it. Even CSIS is officially required to obtain a warrant before intercepting communications.

One concern relating to interception of communications is the lack of fulfillment of the reporting requirements relating to wiretap warrants. All police forces are required to submit to the Justice Department detailed reports outlining how many such warrants were requested and obtained

in a given time period. In fact, many do not bother to submit such reports and those that do frequently fail to report accurate numbers. The audit procedures for this procedural requirement are lax, so there is no reason to suspect this situation will change.

In fact, police investigation powers relating to lawful access are being expanded and this trend is likely to continue. Exceptions to the general principles outlined above have been initiated through new laws and are likely to change the law in recently proposed amendments described below.

New Laws for Lawful Access

In response to the September 11, 2001 terrorist attacks in the United States, the Canadian government attempted to rapidly pass several laws to increase access to private communications by government actors. There was much debate in Parliament regarding the scope of many proposed new laws and, in the end some of the most privacy invasive provisions were abandoned. Still, the government did pass the *Public Safety Act* and the *Anti-Terrorism Act.*

The *Public Safety Act* allows the sharing of airline and other traveler information among certain security agencies for limited purposes including the apprehension of serious criminals or terrorists. In promoting the Bill on its Web site, the Department of the Solicitor General for Canada states, "this is not a power grab." The claim does little to calm the fears of privacy advocates who recognize that all the other "benefits" describing the Act fail to provide any evidence that the increased access will have any effect on public safety.

The *Anti-Terrorism Act* allows the Attorney General to exclude records from the Access to Information Act and stop to any investigations by the Information Commission that deal with these records. This is entirely a discretionary matter for the Attorney General, meaning he may choose to do so or not as he chooses, without requiring outside approval and without consequences.

Lawful Access and International Obligations

The government also signed the Council of Europe's *Convention on Cybercrime*, which may drastically change the scope of police powers relating to access to private communications. For the Convention to be ratified, certain amendments to the Criminal Code must be approved. These amendments would allow law enforcement to require Internet service providers ("ISPs") to retain and collect communications data on their customers. While the data could only be accessed by authorized law enforcement personnel after producing a warrant, the problems with this new law involve both business challenges and privacy risks.

ISPs fear the requirements will be devastatingly costly, requiring several millions of dollars in upgrades cumulatively, according to market estimates. The government has guaranteed ISPs that the costs for the new infrastructure will not be borne by either industry or the Canadian public. This appears to be a hollow guarantee since it must inevitably be paid by businesses (to upgrade their systems) or by taxpayer dollars. If it is paid by businesses, it will inevitably be passed on to their customers, and it may result in Canadian ISPs being unable to compete in a global market against overseas ISPs that are not subject to such requirements.

Further, proper implementation would be exorbitantly expensive, requiring:

- Vastly increased database storage;
- Vastly increased manpower to administer all the different types of files;
- The ability to distinguish specified information from other information without accessing it (presumably impossible);
- Hierarchies of protection, ensuring extremely limited access to the databases;
- Oversight body to ensure only specified information is collected; and
- Methodologies for safe disposal.

Improper implementation means the collected information will be insecurely safeguarded by private ISPs. Thus there will inevitably be infringements on basic privacy rights, leading to improper access to personal information, financial information, health information, corporate information and more. There is concern that this insecurity will lead to individuals and companies being placed in physical and financial dangers.

Technology Changes Scope of Information Access

Privacy advocates warn that the scope of information that can be determined from Internet messages is far more extensive than the simple addresses of the sender and receiver. This concern extends to other forms of communications, including telephone calls. There are different types of warrants that may be granted under the *Criminal Code* and some limit the information to call identifying information (a "DNR"). If an individual is conducting telephone banking, this warrant would show not only the telephone number called, but also the individual's bank account number, personal identification number (PIN), and details of

any financial transaction.

Cellular traffic inevitably shows the number dialed along with information that demonstrates the general location from where the call is made, the duration of the call and the direction in which the caller was traveling. This is clearly not within the scope of the warrant but would inevitably be caught because existing technology cannot easily distinguish call-identifying information from other digital content.

In the end, the problem is that the government appears to be proceeding with this legislation before it has answered many important questions. How will it limit access to information that is not specifically defined in a warrant but is inevitably accessible because of the nature of the technology? How will it define to whom this will apply in order to avoid requiring a small ISP to add prohibitively expensive infrastructure? How can it ensure uniformity of application if there are exceptions for small ISPs? Finally, the government has not demonstrated any specific need for this new legislation beyond the desire to fulfill an international obligation, an obligation that caused serious debate and much dissent in Europe. Despite requests from privacy advocates, there is no evidence to show that existing laws relating to wiretaps and warrants have been insufficient in any specific cases to warrant yet another privacy compromise.

Transparency of Government

Transparency of government activities is necessary to ensure government actors behave honestly and honour the public's confidence in them. Procedures are built into Canadian legislation to ensure Canadians have the right to learn how the government spends money and how much money government representatives are paid (the *Access to Information Act* and others). Further, various committees and special counselors are charged with the responsibility to oversee actions of government bodies and actors.

In some instances, it is clear that the procedures are necessary to avoid conflicts of interest and even improper activities. A situation occurred in which a Canadian Parliament Minister participated in Parliamentary deliberations relating to a tainted blood scandal despite the fact that he had been financially connected to (and benefited from the relationship with) one of the blood suppliers involved. Both the Information Commissioner and the Parliamentary Ethics Counsellor began investigations into the potential conflict of interest. However only the Ethics Counsellor received copies of requested documents while the Information Minister was told the records "could not be located". The Minister was not implicated in the hiding of the records, but this incident demonstrated the need for staff to have clear training in procedures as well as ethics relating to access to information.

Conflicts

Privacy rights conflict with many other desirable goals. A few of the more obvious ones are:

- **Freedom of Access to Information** — the right to learn what others have said about you conflicts with the right of individuals not to have their conversations and correspondence monitored and disclosed. There is a conflict for provincial information and privacy commissioners when these cases arise, as they have the dual duty to protect the public by ensuring information is accessible and to protect individuals to ensure their privacy is protected.

- **Measurement techniques** — it is difficult to determine the extent to which privacy has been protected without some form of audit. For this audit to be effective it must ask invasive questions about privacy infractions.

- **International Obligations** — as we discuss earlier in this report, the dependence on international trade often leads Canadian politicians to agree to treaties and other obligations that threaten Canada's sovereign powers in order to maintain important trade and commerce links.

- **National Security** — this may be illusory, however politicians have been using the threat of terrorism to try to limit and eliminate privacy rights, as described below.

Policy Versus Effectiveness — Creating Policy in Response to Fear

Conflicts are driven by opposing viewpoints, but they may also occur due to political positioning and lack of understanding.

Politicians see the political necessity of responding to the specter of terrorism by quickly enacting security-based legislation. Unfortunately, the effectiveness of such legislation to meet its objectives is rarely evident. In the rush to be seen as "doing something" politicians can create policy that is ineffectual or even harmful to their citizens. The effect can be devastating on Canadian rights and freedoms, while also being ineffectual on the threat that supposedly necessitated the new laws in the first place.

Experts on terrorism state that the behaviour of individual terrorists cannot be predicted, and that terrorists are specifically trained to identify and exploit holes in the system, no matter what laws are in place. Thus, current and proposed anti-terrorist legislation and measures in Canada are likely to prove useless in countering terrorism, but efficient in invading the rights and freedoms of Canadians.

Some claim the push to enact privacy invasive measures is more sinister, and is part of a systematic plan to create a police state in Canada, where the government will have constant access to all activities of citizens. Whether the motives for such measures are merely political or more ominous, the effect is the same. The proposed privacy invasive measures will diminish established Canadian rights and freedoms and have a chilling effect on the populace.

Privacy Enhancing Versus Privacy Invasive — Technology as the Ultimate Solution

As any technology is developed, the abuse of that technology is not far behind. For example, e-mail is widely used and enjoyed by millions of Canadians. It is a so-called "killer-app" of the Internet. The negative outgrowths are spam, e-mail-based frauds financial scams, and hacking by e-mail.

Centralized databases and identification cards offer a more efficient manner to administer social programs. The very existence of such centralized sources of personal information, however, puts individual Canadians at risk from criminals who may access the information illegally; government actors with legal access to the information that may use the information improperly; and the system itself that may not sufficiently protect its information. There is also the very real risk of errors that cause individuals to be denied their rights as citizens.

Since Canada has more social programs than the United States (for example, Canada has universal health care and a higher level of other social assistance programs), Canadians have more opportunities to be listed on government databases than do their American counterparts. This is ironic since the very social programs that were designed and implemented to protect Canadians may now be leading to increased privacy intrusions, confidentially breaches and other security problems

Privacy Invasive Measures as a "Feature"

Frequently, the use of a new technology or the development of a policy is proposed, citing the benefit it will have for users. In considering measures that are privacy invasive, it is more likely than for other technologies and policies that its privacy invasive nature will be recognized and explained. For example, news stories touted the benefits of

implanting RFID chips in children, the elderly and convicts as a security measure, completely ignoring the offence to one's personal liberty and privacy. It also ignored the fact that such chips are designed to remain in the body for life.

In another example, Canadian Immigration Minister Dennis Coderre has called for the development of a national identification card, stating that it would be expedient for Canadians traveling to the United States because the US will soon require more than a Driver's License for Canadian citizens crossing its borders. This argument completely ignores the fact that the ID card would be used for other purposes within Canada, and the fact that Canadians who wish to travel to the US need only show a passport, which is readily available already. Since Canadian Driver's Licenses can still be used in conjunction with a matching provincial birth certificate or a naturalization card, the argument that a National ID card is needed "to combat terrorism" is clearly motivated by other factors.

The Immigration Minister countered that the card would *protect* privacy and help fight identity theft by including fingerprints and other biometrics that would be collected in a central database. Of course, this argument ignores the potential dangers of abuses by the state and by anyone else who gains access to this central database by any means.

He also ignores the likelihood that law enforcement agencies can use this database to target innocent individuals that may engage in legal activities police consider suspect. A typical example is a 52-year-old man who travels to Thailand frequently may do so to support his business interests, but the database would likely target him as a suspected pedophile, and this suspicion would be shared with all government agencies who would start files on him to monitor his e-mail, Internet usage, bank accounts and credit cards. As we have discussed, the problem with shared databases is that information is virtually impossible to remove from all parts of it once it is recorded.

In this way, policy developers behave like marketers of computer software that have notoriously spun problems with their technology as a "feature".

Privacy Versus Compelling Public Interest — Releasing Census Data

A controversy arose over whether to release the data collected in the 1906 Census. Since the first census was taken in 1871, enumerators (those administering the census) took an oath of secrecy and respondents were assured that their personal information would be revealed only to those doing the census work. This was further clarified in the 1918 Statistics Act. However in the Privacy Act, a 92-year rule was established allowing government-collected information to be released after the passage of 92 years.

The concern was that, if the laws relating to revealing information could be changed retroactively then how could Canadians trust that any of their information would be protected? A panel composed of policy-makers, lawyers, historians, genealogists and privacy advocates considered the issues and concluded that 92 years is sufficient to allay privacy concerns, stating the "passage of time diminishes concerns about individual privacy." They also justified the decision to release the data on the basis that the words "perpetual" and "eternal" were not used in giving the assurance of privacy so no long-term guarantee was made.

In reviewing the Panel's decision it appeared that they were trying to fit the facts to justify their decision, instead of making a decision based on the facts. The justification was weak, simply giving the explanation that "we weighed all the facts" and decided to release the data.

Summation and Future Trends

Privacy policy in Canada is based around a few simple fair information principles, stating that organizations:

- Must obtain consent before collecting information;
- Can only collect information that is specific to the particular transaction, and only by fair and lawful means, and the retention, use and disclosure must be limited to that which is necessary for that particular purpose;
- Must explain why collecting the information is necessary, how the information will be used and who will have access to the information;
- Must institute proper and appropriate safeguards to ensure the collected information is secure from unauthorized access — the organization is accountable to ensure these safeguards are instituted; and
- Must ensure their policies and practices are open to the public, and individual information is made available to the individual that provided the information upon request.

Specific exceptions exist for law enforcement, matters of national security, scholarly research, and emergencies. Still, the principle of minimization of information collection requires that, even in these situations, the organization should collect the least personal information necessary, and collect it by using the least privacy-invasive method available.

Finally, the basic legal principle of reasonableness requires that privacy must be protected in the manner that would be expected by the reasonable man (or woman).

The problem in Canada is that these principles are not necessarily followed through in practice. Often this is due to a large and badly coordinated bureaucracy that implements policies without thinking them through to their logical conclusions. There are many examples of this problem, including:

- The requirement of government departments to fulfill privacy impact assessments prior to beginning a project without the requirement to use them or continue to assess the impact on privacy of a project as it continues to be developed;
- Requiring reports on police wiretapping without an audit procedure to ensure the reports are filed and are accurate; and
- Giving privacy commissioners the right to investigate infractions of privacy legislation without the legal authority to enforce privacy laws.

Trends in Public Attitudes

It cannot be ignored that most personal information is given voluntarily by individuals, as opposed to being stolen from them or through forced access. Typically, individuals trade their information in a private transaction, in exchange for the ability to do business at a particular location, or in exchange for other offered benefits. In a capitalist society, individuals are entitled to request virtually anything in exchange for their goods, as long as the other party has no obligation to accept the transaction. In other words, Canadians are able to protect their privacy in the private sector but usually choose not to do so. Most Canadians likely believe this information will be deleted when the contest (or other time-specific activity) has been completed.

The problem with this scenario is that most Canadians are insufficiently informed about the implications of sharing their personal information. They presume it will be used only for the specific transaction or to allow the party with whom they are transacting to contact them. They are generally unaware that their information will almost invariably be sold or shared with many other parties.

It is interesting to note that information about risks to personal privacy and corresponding rights and solutions are widely available to the general public. The various privacy commissioners and activist organizations have hundreds of pages of easy to understand documents available in print form or on their Web sites. Journalists write about the risk that Canada could become a totalitarian state if governmental policies regarding surveillance and access to personal information go unchecked. The number of incidents of identity theft in Canada is rising dramatically. Despite these facts, Canadians are largely ignorant about personal privacy risks, and silent about their privacy rights.

If asked, they say that privacy is important to them. However, many in the privacy community believe that this cannot be true based on the actions (or inaction) of the Canadian people.

Why Are Canadians Uninvolved in Privacy Issues?

In fact, it is likely that privacy is important to Canadians but most do not believe the warnings about what might happen in the future. They have never experienced a perceptible loss of privacy in Canada and the warnings of an impending Orwellian *1984*-like society have been repeated for decades. Canadians still feel that they live in a relatively safe country where their rights are respected. They do

not have to "show their papers" to any police officer who stops them. They may prefer that corporations did not annoy them with so much direct marketing, but they also willingly participate in shoppers' and third party loyalty card programs that require them to give out some very personal information in exchange for discounts and prizes.

Most Canadians do not believe the government is watching them, both because they do not believe it is part of the government agenda and because they do not believe the government is sufficiently competent to do so. They have a greater fear of the US government obtaining access to the personal information of Canadians because the US government *is* considered better equipped and more likely to engage in spying on citizens of any country, including its own.

Indeed, the record of privacy abuses by the Canadian government is more due to sloppy procedures and lack of follow up than to malicious intent or design. Privacy Impact Assessments are done because they must be completed before funding comes through — there is no attempt to make them effective in creating a more privacy conscious project. Law enforcement agencies are required to report on all wiretaps conducted but frequently do not bother to do so and not one bothers to audit the situation — they are probably not trying to hide anything, they just have other things to do.

Privacy Chernobyl

Many in the privacy community believe it will take a serious event to raise the awareness of the Canadian public and instigate a change in public policy. Many have called this galvanizing event a "Privacy Chernobyl".

Whether this event takes place is a matter of guesswork. We cannot predict an act of terrorism or gross incompetence. It is significant, however, that the direction of the change in public policy will likely depend on the details of event. If such an event can be traced back to a situation where better governmental access to personal information could have prevented it, then policies will likely be pushed forth that will erode privacy protections. If an event demonstrates the dangers in widespread collection to personal information (such as the loss of a database leading to individuals being stalked, defrauded or killed) then policies will likely be developed to require better privacy enhancing technologies and less data collection.

Trends in Medical Privacy and Technology

The use of Electronic Medical Records (EMRs) will increase due to the expediency of using such systems. Indeed, there will likely be a serious push to create a nationwide database of EMRs, but this will be slowed if not stopped by conflicts of jurisdiction. Health is a provincial matter as clearly stated in the Constitution, and it will be very difficult to convince provincial governments to give up their power over it.

Trends in International Activities

There is no reason to suspect that sharing of information across the US-Canadian border will diminish. In fact, it is likely to continue and grow under the guise of catch phrases such as "national security", "the fight against international terrorism" and "the war on drug trafficking".

Trends in Legal Activity

Canadian privacy commissioners are becoming increasingly vocal and active in the fight against privacy-invasive policies. This is likely to continue, with privacy commissioners using whatever powers they have to bring the message to Canadians and the Canadian government. Since the powers of the commissioners are limited, they are relegated to educating the public and the government, and, perhaps, bringing more privacy-related legal challenges on behalf of the Canadian people.

Using the Commissioner's power to make matters public has been effective in limited cases, although more frequently the statements of the various commissioners have no obvious effect. Still, in 2000, the federal Privacy Commissioner exposed the existence of a database of personal information of Canadian citizens, contrary to both policy and the mandate of the particular department. It became a minor scandal and the database was disbanded, at least publicly.

Already, the stage has been set for a Constitutional challenge to the CCRA airline travelers' database. The federal Privacy Commissioner presented legal opinions to Parliament by renowned legal experts the Honourable Marc Lalonde, P.C., O.C., Q.C. (a former Canadian Justice Minister), the Honourable Gérard V. La Forest, C.C., Q.C. (a former Justice of the Supreme Court of Canada) and of Mr. Roger Tassé, O.C., Q.C., stating their belief that creation and use of the database gives rise to a legitimate legal challenge under the Charter. Mr. Lalonde cited a Supreme Court case that demonstrated that "the legitimate interests of the State requiring the collection of personal information must be balanced with the fundamental right to privacy of all Canadians."

Other challenges are likely to be brought if legislation for a National ID card is tabled, or in matters of health

privacy, anti-terrorist legislation to implement strategies that do are not proven to have any effect on terrorist activity, and other matters. The results in the courts may not be what the commissioners desire if trends continue. A series of court cases shows the Federal Court being negative and even hostile toward the federal Privacy Commissioner, the federal Information Commissioner, and various provincial information and privacy commissioners. Judges have declared that the courts owe no duty of deference to the Commissioner, and frequently deny the claims of commissioners. Many cases brought by commissioners are denied and appealed by the commissioners.

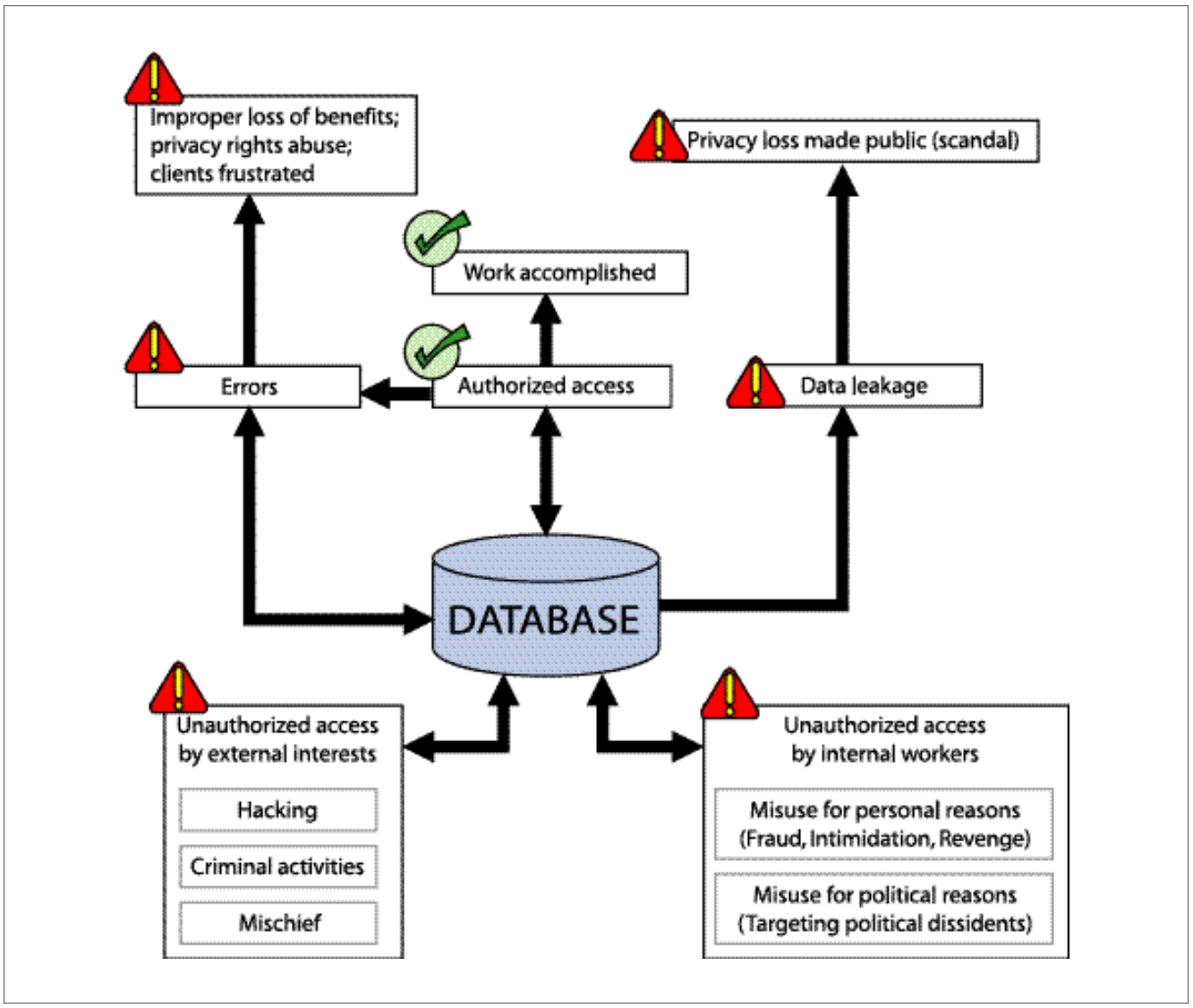
Trends in Commercial Activities

As the public begins to become more aware of privacy issues they will demand more protection of their personal information from corporations. It will become financially prudent to use privacy enhancing technologies in customer databases, e-commerce and other business-related systems. In theory, companies that appear more trustworthy to consumers will garner greater sales than those that appear less trustworthy.

Since it is more efficient and less costly to implement privacy enhancing technologies at the initial design stage, more and more companies will do so. Unlike government departments, businesses must be fiscally responsible or they cannot continue to exist.

Trends in Technology

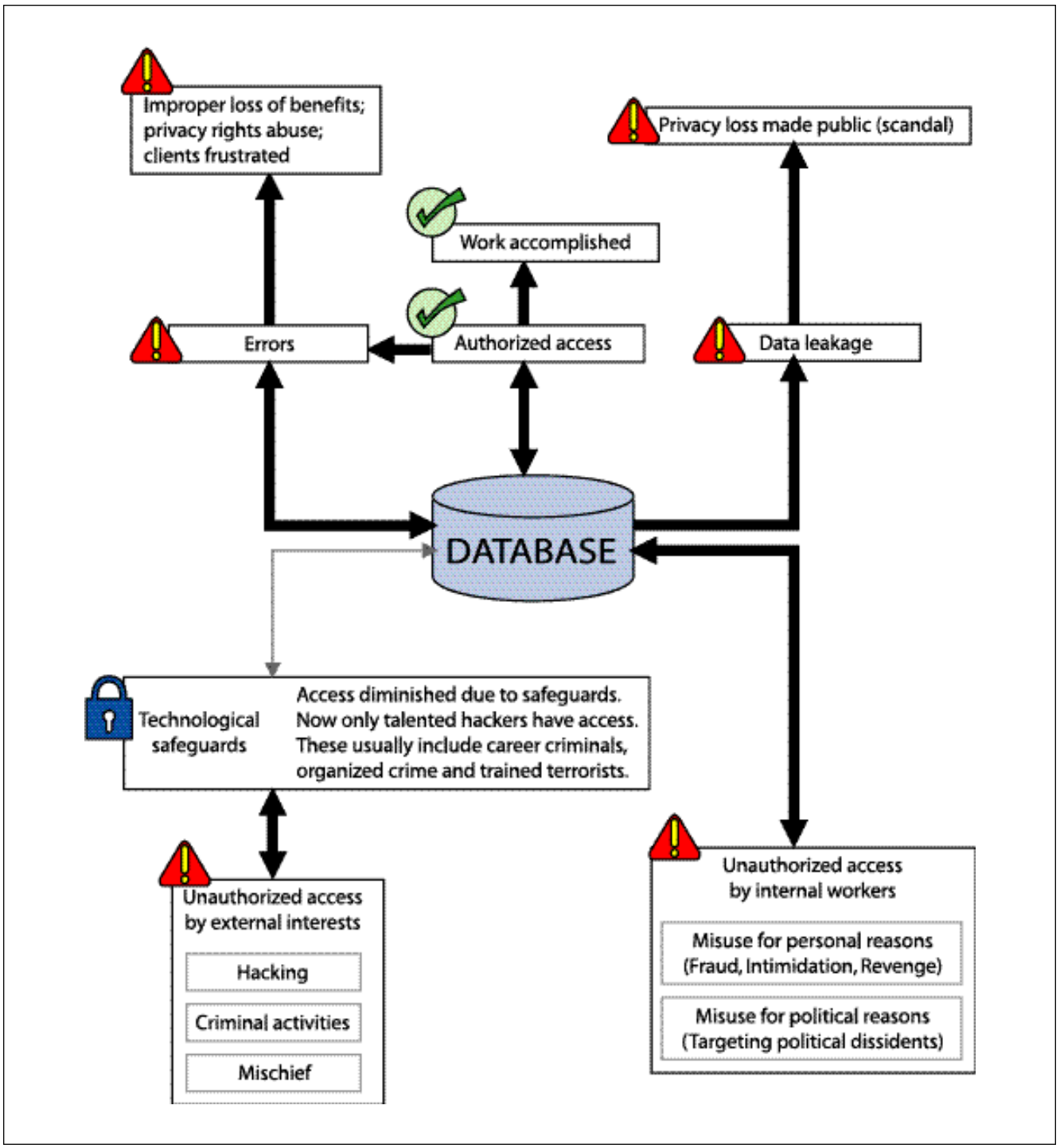
Meanwhile, privacy related technologies will continue to develop and these will be both privacy enhancing and privacy invasive. It is likely that RFID technologies, for example, will be used more frequently on automobiles, computers and other private property as a theft deterrent (or a recovery assistant). The use of RFID to embed tracking devices in humans (so-called “chipping”) will likely be slower to grow. Some individuals may wish to use the devices for their children and elderly relatives for safety purposes, but the highly invasive nature of such devices will make the majority of individuals refrain from obtain-

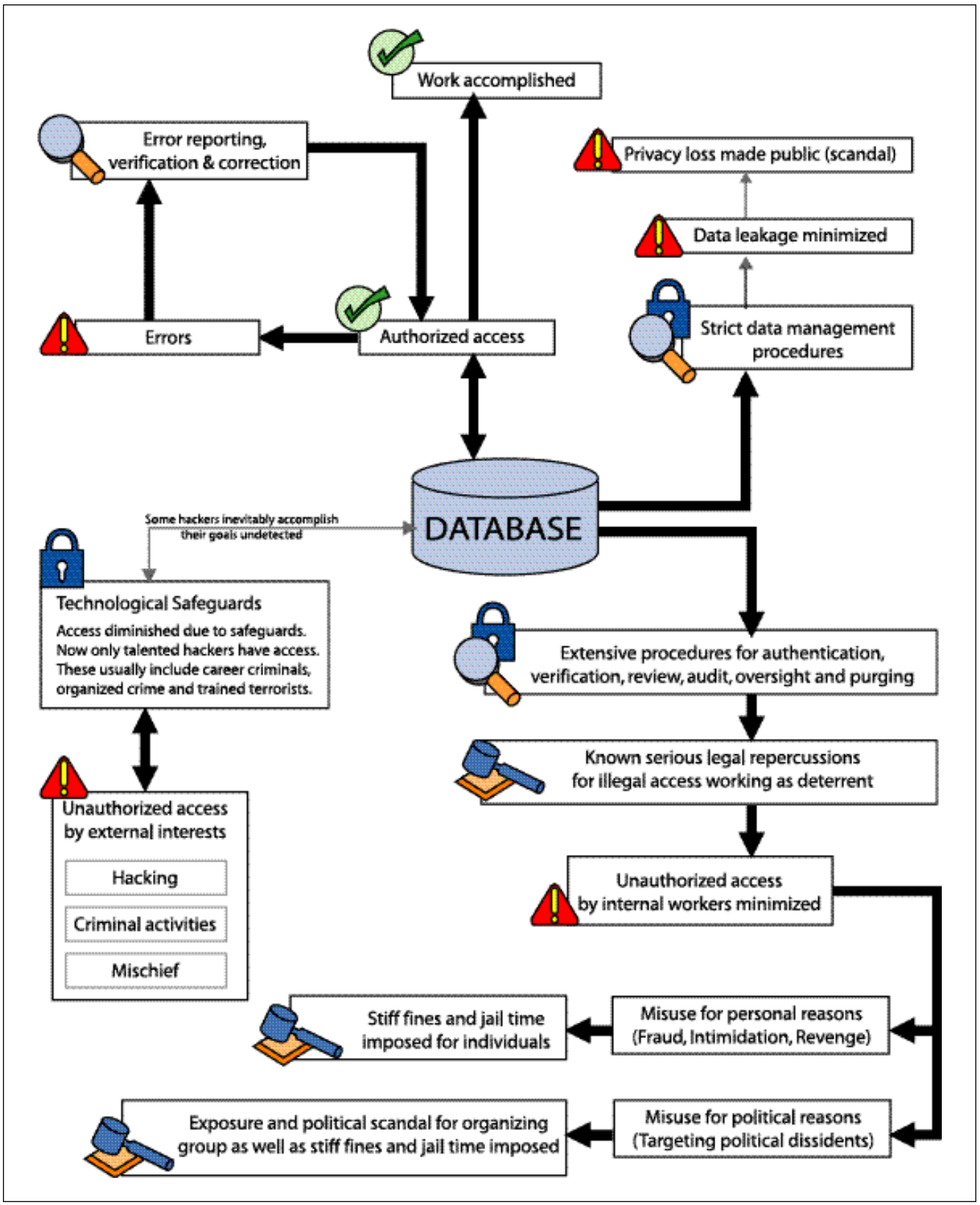


ing such devices for themselves. As “chipped children” grow to adolescence, there is likely to be a backlash by these individuals demanding their privacy rights, and the removal of these devices.

In the public sector, it is important to recognize that technology itself cannot be a solution. Any technology that can be developed can inevitably be circumvented. Any system that relies on human input for administration is error-prone and certainly can be abused. Clearly it is advisable for governments to keep up to date in implementing more efficient methods of record-keeping and better privacy enhancing technologies. But these technologies must be balanced with clear, complete, thoughtful and flexible policies.

The law of large numbers recognizes that in any large enough system there will be errors. Modern software packages that run databases are invariably comprised of millions of lines of programming code, suggesting that errors exist within them. Further, human error is just as likely to occur, and human input brings forth the further likelihood of abuse of the system by individuals. A system to audit and oversee both the systems and the human input is necessary to ensure the systems run smoothly and breaches of personal rights are minimized.




Work accomplished
Error reporting, verification & correction
Privacy loss made public (scandal)
Data leakage minimized
Errors
Authorized access
Strict data management procedures
DATABASE
Some hackers inevitably accomplish their goals undetected
Technological Safeguards
Access diminished due to safeguards. Now only talented hackers have access. These usually include career criminals, organized crime and trained terrorists.
Extensive procedures for authentication, verification, review, audit, oversight and purging
Known serious legal repercussions for illegal access working as deterrent
Unauthorized access by external interests
Hacking
Criminal activities
Mischief
Unauthorized access by internal workers minimized
Stiff fines and jail time imposed for individuals
Misuse for personal reasons (Fraud, Intimidation, Revenge)
Exposure and political scandal for organizing group as well as stiff fines and jail time imposed
Misuse for political reasons (Targeting political dissidents)

Recommendations

In developing policy, any nation must first decide upon fundamental principles. Protection of privacy is necessary to a country that values independence and the right to self-determination. The right to be left alone necessitates that an individual have more control and access to his information than anyone else. If these are serious priorities, then serious measures can be undertaken to protect privacy.

Considering specifics, it must be determined whether or not private information should be gathered at all; if so, what information; who has the right to gather and retain this information; under what circumstances; what are the obligations to protect information and access; what remedies are available if misuse occurs; how can digital rights "function creep" be avoided; and what should be the international role of the country in privacy matters – a leader, a follower, a rejector, or an independent?

Policy must be meaningful and fully thought through to ensure activities are not shams to hide the fact that information is being collected and used at the will of the collector. There must be layers of oversight to ensure fundamental principles are upheld. It is important to have critical mass of people involved for meaningful development of legislation, so it is necessary to educate the public.

It is important to recognize that technology can never be considered a solution in itself. The best Privacy Enhancing Technologies, biometric encryption and data minimization policies are subject to human error. Because of the need for human involvement in processing information, any technology designed to do anything beyond simple recognition will always be subject to unauthorized access.

Elements of a National Privacy Policy

Learning from the Canadian situation, these are the elements we consider important for a public policy of privacy protection to be effective:

1. Central Principle

An overall privacy principle that is enshrined in a national law that over-rides all other laws, such as a Constitution or Charter, outlining the recognition of privacy as an inalienable human right.

2. Privacy Law with Force

A national privacy law to instill powers and responsibilities in an independent, impartial, non-partisan public body, with an independent budget (a Privacy Commission). Powers should be given to conduct investigation, audit, oversight, review, and to impose enforcement including the requirement for specific compliance and the imposition of remedies. The privacy law should be quasi-judicial and the Privacy Commission should have the power to intercede on behalf of the public in courts and in all levels of government. The privacy law should clearly state its primacy over all laws dealing with the collection, use and disclosure of personal information.

The law should include:

- Reporting, review and appeal procedures;
- Investigation and oversight procedures;
- Audit system to ensure policies are fulfilled and "function creep" does not occur;
- Serious mandatory penalties to ensure procedures and measures are carried out.

Balancing this, there should be a justification for exceptions to privacy policy in the interests of national security and safety. However, the audit and oversight body must have meaningful involvement in such exceptions, and the exception process should be conducted in an open and transparent manner, to the maximum degree possible.

Definitions must be both broad and specific, recognizing the changing nature of personal information. Broad principles would protect the spirit of protection of privacy of personal information and specific regulations would define administration. The broad principles should be recognized as primary, and the specific regulations should be relatively easy to update. For example, the very definition of "personal information" varies depending upon the scope of medical technology and biometrics, however the principle ensuring the protection of the privacy of personal information remains, whether it is in the form of photographs, fingerprints or DNA.

3. Include Privacy in Sector Legislation

Enshrine mandatory privacy protection in specific laws and regulation of each sector, including a "substantially similar" clause to ensure uniformity of the application of the laws across the country. Any new and existing laws that permit any collection or use of personal information must implement new privacy clauses by a certain date. These clauses must follow the principles and specify precisely how measures will operate. In particular, measures to safeguard privacy should be included

in legislation relating to financial transactions and banking; employment and workplace regulation; medical and health regulation; and consumer protection.

It is advisable to allow the businesses, organizations and other entities that comprise these sectors extensive involvement in the creation of these clauses and regulations. Indeed, sector involvement should also be extended to the review, audit and oversight procedures. This is to foster a spirit of commitment to the principles — it is recognized that measures are more likely to be understood and conscientiously fulfilled if they are developed and administered by those most affected by them. However, final judgment and enforcement would remain with the Privacy Commission to ensure compliance. Strong penalties must be a significant element of the measures, including a minimum mandatory penalty.

4. Continuity in New Laws

Any new initiative proposed by the government that collects, uses or discloses personal or identifying information under existing laws must conform to the same principles. Compliance relating to such privacy matters should be the right and duty of the Privacy Commission, and new legislation should require a higher majority for passage if it is declared contrary to overall privacy principles by the Privacy Commissioner. This is one of the measures that should be undertaken to ensure meaningful inclusion in the development of legislation.

5. Committee of Experts

The government must be required to respond to requests and concerns of a committee of experts drawn by the Privacy Commissioner of interested parties from academia, business and commerce, public interest groups, and sector-specific interested parties. It should be the duty of the Privacy Commission to foster the development of privacy expertise at specific centers, especially universities and civil organizations.

6. Education

The duty to educate the public on matters of privacy, and to promote the understanding of privacy principles and culture should also be a duty of the Privacy Commission. Related to this is to develop a procedure to continuously educate all levels of civil service on the basic principles of privacy.

7. International Policy

A clear policy must be defined in terms of international obligations and the sharing of personal information. The sharing of such information should be permissible only by treaty and only after conforming to the overall privacy principle, and only when consistent with international human rights law.

Balancing Privacy with Other Important Goals

It is necessary to recognize that privacy is neither the sole nor even the major goal of any nation or administration. It is only one of several fundamental rights and freedoms, and it must be balanced against other legitimate purposes of the nation. In considering the threat of terrorism, biological or medical epidemics, economic devastation through fraudulent and other criminal activities conducted through financial or computer networks, and other threats to a peaceful nation, it must be recognized that privacy may be infringed when doing so can offer a substantial and necessary public good.

The problem is that these recognized evils are used to justify measures that are not proven to have any effect at reducing the problems. Public fear of terror combined with public apathy allows politicians to use terror as an excuse to enact measures that the public does not want or need.

The federal Privacy Commissioner suggested a four-part test before enacting any measure that infringes on or limits privacy:

- It must be demonstrably necessary to meet some specific need;
- It must be demonstrably likely to be effective in achieving its intended purpose;
- The intrusion on privacy must be proportional to the benefit to be derived;
- It must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same goal.

In short, it must show necessity, effectiveness, proportionality and the lack of a less privacy-invasive alternative. This is the principle of minimization. Rather than thinking "what would be the harm in collecting certain data" organizations and governments should be asking themselves, "what would be the benefit, will the benefit be realized through privacy infringement, is the benefit worth the risk and how can the benefit be obtained in a minimally privacy

invasive manner?”

Any nation that values a free and independent citizenry must value individual privacy. It is a fundamental right but difficult to define, and its value is best understood by considering what life would be like without it. The people of Canada rarely express interest or concern for privacy rights, but that is at least partially because they cannot truly imagine life without it. The depiction in stories and entertainment of a totalitarian regime where privacy rights are non-existent does not strike at the heart of most Canadians because they have never experienced it in real life.

There is every indication that government and other initiatives described in this report are leading toward a society that will gradually experience less and less privacy protection. That is, unless the people of Canada begin to value of rights they hardly know they have, and respond by making their wishes known. Recognizing that Canadian behaviour is based on reasonableness, balancing, and avoiding extremes, it is likely that Canadians will eventually recognize the value of the right to privacy and will gradually work their way toward better and more effective policies, systems and laws that improve little by little.

Privacy Commissioner Budgets

The budgets for the federal Privacy Commissioner and for the various provincial and territorial Information and Privacy Commissioners are each determined separately by their particular governments. Generally, the Commissioner presents an estimated or proposed budget, then a Parliamentary (federal) or legislative (provincial and territorial) committee determines and formalizes the budget. The Auditor General for Canada or for each individual province or territory may audit the financial statements of the particular commission either at the request of the Commissioner, under his own discretionary authority or by law — it varies by jurisdiction.

Federal Privacy Commissioner

The budget for the federal Privacy Commissioner is contained within the Annual Report to Parliament.

In brief, the budget for the 2001-2002 fiscal year was $11,457,768 and the budget for the 2000-2001 fiscal year was $8,359,820. It was increased to allow the PC to deal with the effects of PIPEDA.

British Columbia

NOTE: Web site has been changed to www.oipc.bc.ca

The amount for the BC IPC Budget is determined by the Finance and Government Services Committee, made up of members of the Legislative Assembly of BC. This means that the budget for the office is not independent of the government, upon which the IPC reports.

In the 2001-2002 fiscal year, the budget was $2,344,000 and the Committee proposed a 35 percent cut to take effect over 3 years (10 percent in 2002-2003, 10 percent in 2003-2004, and 15 percent in 2004-2005). The proposed budget for 2002-2003 is $2,145,000.

Budgets may be audited by the Auditor General of British Columbia but this is not done automatically. The most recent budget proposal was audited by the Auditor General of British Columbia at the request of the IPC. The request was made because of the diminishing budget in this and previous years.

Ontario

The budget for last year was $7.4 million, divided between Salary and Benefits ($6.2 million) and ODOE ($1.2 million).

The budget is determined in the following manner: The IPC develops an estimate of costs. This estimate is reviewed and approved by the provincial Board of Internal Economy, which is chaired by the Speaker of the House. Once it is approved, it becomes the formal budget. The Commissioner indicated that they have been fortunate to have a good working relationship with the Board and have not had their budget cut the way it was in BC.

The IPC is audited by the Provincial Auditor annually. This usually occurs in May shortly after the fiscal year end adjustments have been processed.

Québec

The budget for the 2001-2002 fiscal year was $4,053,800 and the budget for the 2000-2001 fiscal year was $3,696,900.

Biographies

To research this document, we discussed the principles and practices of privacy in Canada with many individuals, including staff at the various Privacy Commissioner's offices across Canada, academics, privacy activists, and privacy consultants. The following are some of the recognized individuals that provided their opinions and expertise. Their specific statements are not quoted directly as most preferred not to be quoted, however their information is accumulated into our findings.

Dr. Stefan Brands

Dr. Brands is one of the world's leading experts on electronic authentication and privacy-enhancing technologies. His MIT Press book has been widely acclaimed for introducing breakthrough electronic authentication techniques for transaction systems and chipcards. Dr. Brands is currently an adjunct professor at McGill's School of Computer Science in Montréal.

"Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy," August 2000, MIT Press, ISBN 0-262-02491-8. With a foreword by professor Ronald L. Rivest, this 350-page book describes the mathematics of Digital Credentials and analyzes their security. For reviews and excerpts, see http://www.credentica.com/technology/book.html

Dr. Ann Cavoukian

Ph.D. Psychology, Ontario Information and Privacy Commissioner

Recognized as a leading authority on privacy and data protection, Dr. Ann Cavoukian was appointed Information and Privacy Commissioner in 1997. As Commissioner, Cavoukian oversees the operations of Ontario's freedom of information and privacy laws, which apply to both provincial and municipal governments. She serves as an officer of the legislature, independent of the government of the day.

Cavoukian joined the Office of the Information and Privacy Commissioner in 1987, during its start-up phase, as its first Director of Compliance. She was appointed Assistant Commissioner in 1990. Prior to this office, Cavoukian headed the Research Services Branch of the Ministry of the Attorney General, where she was responsible for conducting research on the administration of civil and criminal law. Cavoukian received her M.A. and Ph.D. in Psychology from the University of Toronto, where she specialized in criminology and law, and lectured on psychology and the criminal justice system.

Increasingly in the public eye, Cavoukian's expertise has been sought out by industry and media alike. She is particularly interested in advancing privacy protection through the pursuit of privacy-enhancing technologies and has been involved in a number of committees focused on privacy and technology, including the World Wide Web Consortium's P3P (Platform for Privacy Preferences) initiative. She has also served as a member of the American Task Force on Privacy, Technology and Criminal Justice Information.

Cavoukian is frequently called upon to speak at leading forums around the world. Her published works include a book entitled *Who Knows: Safeguarding Your Privacy in a Networked World* (McGraw-Hill, 1996) and most recently, The Privacy Payoff (McGraw-Hill Ryerson, 2002), in which she and the book's co-author, journalist Tyler Hamilton, address how successful businesses build customer trust.

Dr. Andrew Clement

B.Sc. Mathematics (Honours) (University of British Columbia), M.Sc. Computer Science (University of British Columbia), Ph.D. Computer Science (University of Toronto), Associate Professor

Dr. Andrew Clement is an Associate Professor in the Faculty of Information Studies at the University of Toronto, holding a cross-appointment in the Department of Computer Science at the University of Toronto.

Clement coordinates the Information Policy Research Program, and is active in the Information Highway Working Group, a coalition of public interest groups which seeks to ensure that citizens' interests and needs are a primary focus in the public policy debate around Canada's 'Information Highway'. As well, he is the principal investigator of a 3-year SSHRC strategic grant entitled "Developing Information Policies for Canada's 'Information Infrastructure': Public Interest Perspectives" (DIPCII). Finally, he chairs the Working Group on Computers and Work (WG9.1) of the International Federation for Information Processing (IFIP).

Michael A. Geist

LL.B. (Osgoode), LL.M. (Cambridge), LL.M. (Columbia), J.S.D. (Columbia), Associate Professor

Dr. Michael Geist is an associate law professor at the University of Ottawa specializing in Internet and e-commerce law and serves as Technology Counsel to Osler, Hoskin & Harcourt LLP. He has obtained a Bachelor of Laws (LL.B.)

degree from Osgoode Hall Law School in Toronto, Master of Laws (LL.M.) degrees from Cambridge University in the UK and Columbia Law School in New York, and a Doctorate in Law (J.S.D.) from Columbia Law School.

Dr. Geist has written numerous academic articles and government reports on the Internet and law, is national columnist on cyberlaw issues for the Globe and Mail, the creator and consulting editor of BNA's Internet Law News, a daily Internet law news service, editor of the monthly newsletter, Internet and E-commerce Law in Canada (Butterworths), the founder of the Ontario Research Network for E-commerce, on the advisory boards of several leading Internet law publications including Electronic Commerce & Law Report (BNA), the Journal of Internet Law (Aspen) and Internet Law and Business (Computer Law Reporter) as well as the author of the textbook Internet Law in Canada (Captus Press) which is now in its third edition. Dr. Geist serves on the director and advisory boards of several Internet and IT law organizations including the Canadian Internet Registration Authority, the dot-ca administrative agency, the Canadian IT Law Association, Watchfire, and Verifia. He is regularly quoted in the national and international media on Internet law issues and has appeared before government committees on e-commerce policy. More information can be obtained at http://www.lawbytes.ca.

Peter Hope-Tindall

Peter Hope-Tindall is Technical Director and Chief Privacy Architect of dataPrivacy Partners Ltd., one of Canada's leading privacy consulting firms. Formerly, he was special advisor to the Information and Privacy Commissioner/Ontario for biometrics and cryptography where he conducted privacy audits and assessments and monitored the development of large government systems having a significant privacy component. Mr. Hope-Tindall also represented the province of Ontario at Industry Canada's 1998 encryption policy round-table from which the template for Canada's National Encryption Policy arose.

Mr. Hope-Tindall recently completed an engagement as Privacy Architect to the Government of Ontario Smart Card project, a challenging assignment to address the imperative of security within a privacy framework. His current research interests include development of an effective privacy metric to allow objective choices to be made and options considered within a given system design. The metric will also provide a framework for establishing the on going effectiveness of privacy policies and technology, post implementation.

Ian R. Kerr

Canada Research Chair in Ethics, Law & Technology B.Sc. (Alberta), B.A. (Hons.) (Alberta), M.A. (U.W.O.), LL.B. (U.W.O), Ph.D. (Philosophy of Law) (U.W.O), of the Bar of Ontario, Associate Professor

Prior to his appointment at the University of Ottawa, Ian Kerr was jointly appointed to the Faculty of Law, the Faculty of Information & Media Studies and the Department of Philosophy at the University of Western Ontario. He is a past recipient of the Bank of Nova Scotia *Award of Excellence in Undergraduate Teaching*, the University of Western Ontario's Faculty of Graduate Studies' *Award of Teaching Excellence, the Professor of the Year* at Western's Faculty of Law, as well as several prestigious fellowships and research grants. Professor Kerr currently teaches in the areas of Internet Law, Law & Technology, Contract Law, and Legal Theory.

His primary areas of interest lie at the intersection of Media, Technology, Private Law and Applied Ethics. He has published writings in academic books and journals on Ethics and Electronic Information, Internet Regulation, E-Commerce, Internet Service Providers, Online Defamation, Pre-natal Injuries, Unwanted Pregnancies, and the Judicial Use of Legal Fictions. His current program of research focuses on electronic commerce and other legal and ethical issues in multi-media, including work on Internet service provider liability, the ethics of automation, the legal ramifications for businesses who use automated software devices, contract formation in cyberspace, and online defamation.

Dr. Kerr is a member of the Law Society of Upper Canada, The Canadian Association of Law Teachers, The Canadian Bar Association, and the Uniform Law Commission of Canada's Special Working Group on Electronic Commerce. He sits as a member on the Advisory Board for Butterworths' *Canadian Internet and E-Commerce Law Newsletter* and is co-writing a textbook for Prentice Hall on *The Legal Aspects of Doing Business.*

Richard Owens

B.A., with High Honours (McGill), J.D. (University of Toronto), partner with Smith Lyons 1987-2001

Richard Owens has been the Executive Director of the Centre for Innovation Law and Policy since February 2001. He graduated from the University of Toronto Law School in 1987 and was called to the bar in 1989. He then built a very successful career as a partner with Smith

Lyons (now Gowlings) LLP practicing corporate and commercial law and specializing in technology related law, leading its IT and IP practices.

Owens has acted for many high-technology companies as well as financial institutions in their uses of technology, including licensing, strategic alliances and joint ventures, privacy, financing, outsourcing, electronic commerce, public/private partnerships, and Internet issues. He is a member of many organizations, including the International Bar Association, the Canadian IT Law Association and the Computer Law Association. He is a director of the Computer Law Association and of other private corporations.

Owens was recognized as one of Canada's leading computer lawyers in the 1999, 2000 & 2001 Leading Lawyers in Canada Guides, published jointly by Lexpert and American Lawyer magazine. He has written and published widely on the law of information technology, privacy, and the regulation of financial institutions. As an adjunct professor at the University of Toronto, Richard has taught a course called the Law of Information Technology and Electronic Commerce, and now teaches another course on Innovation Law and Policy. He is currently at work on several projects relating to innovation law and policy.

Stephanie Perrin

M.A. English

As the former Chief Privacy Officer of Zero-Knowledge Systems, a privacy technology solutions company, Perrin developed policy and management systems to implement privacy objectives within the company, and provided advice and analysis of customer needs and requirements for enterprise and consumer products and services. Active in domestic and international privacy policy and compliance fora, including the International Association of Privacy Officers and the Canadian Council of Chief Privacy Officers, she is in great demand as a speaker on privacy policy and compliance issues.

Perrin was instrumental in developing Canada's privacy and cryptography policies for over fifteen years. Formerly the Director of Privacy Policy for Industry Canada's Electronic Commerce Task Force, she led the legislative initiative at Industry Canada that resulted in the Personal Information Protection and Electronic Documents Act, privacy legislation that came into force in 2001 and has set the standard for private sector compliance. She is the principal author of a text on the Act, published by Irwin Law.

From 1991 until 1999 she represented Industry Canada on the Canadian Standards Association's technical committee on privacy, and was a member of the drafting committee that developed CAN/CSA–Q830-96, the Model Code for the Protection of Personal Information. She was a member of the Ad Hoc Advisory Committee of ISO that examined the utility of developing a management standard for the protection of personal information in 1997-98. She represented Canada internationally at the OECD Security and Privacy Committee for many years and led Canada's delegation to the ad hoc working group that developed the OECD Cryptography Policy Guidelines.

In the early eighties, Perrin was one of Canada's first Freedom of Information and Privacy Officers, and was the first President of the professional association, the Canadian Access and Privacy Association.

Caryn Mladen – Short Bio

Caryn Mladen is a business consultant, writer, and instructor whose work focuses on the digital communications industry, especially matters of privacy and security. Her clients range from large multinational corporations to small boutique firms. She has been an intellectual property lawyer, co-chief editor of America Online's print publication Multimedia Online and co-author of the best-selling books Making Money with Multimedia and multiple editions of The Canadian Computer Handbook. Her latest co-authored book is University Planning for Canadians for Dummies and her next Dummies book is set to release to the US market in August 2003. Caryn has written hundreds of articles and columns dealing with technology, business, education, and privacy. Her articles and interviews have been translated into French, Spanish, Italian, Hungarian, Russian, Japanese and other languages.

In December 2001, Caryn co-founded a non-profit initiative called Privaterra, devoted to providing privacy and security technology training and support to human rights workers worldwide. As a director of this international non-governmental organization, she educates the public about privacy and security issues by speaking to the media and publicly at conferences and universities, including Stanford and Berkeley. Caryn has spoken at such conferences as Comdex and MacWorld, and on Canadian television and radio news programs for the CBC, WTN, CITYtv, and CTV.

Contact: Caryn@privaterra.org
Telephone: 416-816-7010
Fax: 416-463-3648
Address: 128 Danforth Avenue, Suite 210, Toronto, ON, Canada, M4K 1N1

Bibliography

In preparing this report, we considered various materials on Web sites of Privacy Commissioners across Canada, HRDC, Industry Canada, Supreme Court of Canada, various news agencies activists, and the National Privacy Coalition mailing list. The list provided below includes some of the major reports that may provide further background and insight.

Privacy Legislation and Reports

The Personal Information and Electronic Documents Act, An Annotated Guide
Stephanie Perrin, Heather H. Black, David H. Flaherty and T. Murray Rankin
ISBN: 1-55221-046-4

The Privacy Commissioner of Canada's 2001-2002 Annual Report to Parliament
www.privcom.gc.ca/information/ar/02_04_10_e.pdf
All previous annual reports are available at
www.privcom.gc.ca/information/ar/02_04_e.asp

Privacy Act Reform: Issue Identification and Review — A Report by the Privacy Commissioner of Canada on Proposed Amendments to the Federal Privacy Act (June 16 2000) — not available online but referenced in 1999-2000 Annual Report of the Federal Privacy Commissioner
Report of the Expert Panel on Access to Historical Census Records
www.statcan.ca/english/census96/finalrep.htm

International Materials

Privacy and Human Rights 2002
Annual survey by Electronic Privacy Information Center
www.epic.org/bookstore/phr2002/

Global Privacy Law: A Survey of 15 Major Jurisdictions by White & Case LLP
Prepared for 2002 Global Privacy Symposium, April 30, 2002
www.whitecase.com/report_global_privacy.pdf

Initiative on Privacy Standardization in Europe by the CEN/ISSS IPSE working group
February 13, 2002
www.cenorm.be/isss/Projects/DataProtection/IPSE/ipse_finalreport.pdf

Part of the forthcoming work by Colin Bennett with Charles D. Raab
The Governance of Privacy: Policy Instruments in Global Perspective (London: Ashgate Press, forthcoming)
A chapter from that book was presented at the Cardiff Data Protection Commissioners Conference in September 2002 and only Bennett's powerpoint presentation, rather than his paper, is available online at:
www.informationrights2002.org/presentations/bennet_Workshop_9.ppt
More information is available at his personal website is at
web.uvic.ca/~polisci/bennett/index.htm

Medical Privacy

Canadian Medical Association (CMA), Health Information Privacy Code
http://www.cma.ca/cma/common/displayPage.do?pageId=/staticContent/HTML/N0/l2/inside/policy-base/1998/09-16.htm

Romanow, Roy, Building on Values: The Future of Health Care in Canada, Commission on the Future of Health Care in

Canada, November 2002.
http://www.healthcarecommission.ca/pdf/HCC_Final_Report

The Health of Canadians — The Federal Role: Final Report on the state of the health care system in Canada
Chair: The Honourable Michael J. L. Kirby Deputy Chair: The Honourable Marjory LeBreton October 2002
http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-e/soci-e/rep-e/repoct02vol6-e.pdf

Medical Record Privacy
Electronic Privacy Information Center
http://www.epic.org/privacy/medical/

Patient Privacy in the Information Age
Speech by Privacy Commissioner of Canada at E-Health 2001: The Future of Health Care in Canada, May 29, 2001
http://www.privcom.gc.ca/speech/02_05_a_010529_e.asp

Protection of Personal Health Information
Information and Communications Technologies in Health
Office of Health and the Information Highway (OHIH), Health Canada
http://www.hc-sc.gc.ca/ohih-bsi/theme/priv/index_e.html

Information and Communications Technologies in Health
Office of Health and the Information Highway (OHIH), Health Canada
http://www.hc-sc.gc.ca/ohih-bsi/theme/ehr_dse/index_e.html

White-Paper: Selected Legal Issues in Genetic Testing: Guidance from Human Rights
Health Canada — Applied Research and Analysis Directorate (ARAD)
http://www.hc-sc.gc.ca/iacb-dgiac/arad-draa/english/rmdd/wpapers/jones.pdf

Towards Electronic Health Records
Office of Health and the Information Highway, Health Canada
http://www.hc-sc.gc.ca/ohih-bsi/pubs/2001_ehr_dse/ehr_dse_e.pdf

Secondary Use of Personal Information in Health Research: Case Studies,
Canadian Institutes of Health Research
http://www.cihr-irsc.gc.ca/publications/ethics/privacy/case_studies_nov2002_e.shtml

Smart Health Cards: An Unavoidable Public Debate
Observ@tions — Bulletin of the Telehealth Ethics Observatory
Vol. 3, No. 1, May 31, 2001
Centre for Bioethics, Clinical Research Institute of Montreal
http://www.ircm.qc.ca/bioethique/english/telehealth/archives/issue31.html#smart

Privacy Horizon — Brendan Seaton’s monthly eZine of health privacy news.
http://www.ehealthprivacy.com/privacyhorizon/

Privacy Enhancing Technologies

Information and Communications Technologies in Health
Office of Health and the Information Highway (OHIH), Health Canada
http://www.hc-sc.gc.ca/ohih-bsi/theme/ehr_dse/index_e.html

Information and privacy Commissioner/Ontario
Biometrics and Policing: Comments from a Privacy Perspective
August 1999
http://www.ipc.on.ca/docs/biometric.pdf
This is a chapter, contributed by Ontario Information and Privacy Commissioner Ann Cavoukian to the book, Polizei und Datenschutz — Neupositionierung im Zeichen der Informationsgesellschaft, a compilation of essays by international privacy and data protection experts. The book was released in conjunction with the Data Protection Authority of Schleswig-Holstein's 1999 Summer Academy. This theme of the conference was Police and Data Protection. Released August 1999.

Privacy Technology Review
Office of Health and the Information Highway, Health Canada
http://www.hc-sc.gc.ca/ohih-bsi/pubs/2001_tech/tech_e.html

Privacy Impact Assessments

Privacy Impact Assessment Policy
Treasury Board of Canada Secretarait
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp
(This policy applies to all government institutions listed in the Schedule to the Privacy Act, except the Bank of Canada.)

Privacy Impact Assessment — Obligation or Opportunity, The Choice is Ours!
Peter Hope-Tindall, dataPrivacy Partners
2000-2002, Prepared for the CSE ITS Conference, Ottawa, Ontario, May 16, 2002

Public Key Infrastructure

Government of Canada Public-Key Infrastructure (PKI)
Treasury Board of Canada — Secretariat
www.cio-dpi.gc.ca/pki-icp/gocpki/gocpki_e.asp

Rethinking Public Key Infrastructures and Digital Certificates — Building in Privacy
Stefan A. Brands, MIT Press, Cambridge (USA) 2000

Social Insurance Number

Beyond the Numbers: The Future of the Social Insurance Number in Canada Report of the Standing Committee on Human Resources Development and the Status of Persons with Disabilities
Albina Guarnieri, M.P., Chair, May 1999
www.parl.gc.ca/InfoComDoc/36/1/HRPD/Studies/Reports/hrpdrp04-e.htm

Address to the Canadian Information Technology Security Symposium Audit and Privacy Issues — Policy Regarding SINs in Canada
Brian Foran, Director, Issues Management & Assessment, Privacy Commission of Canada
Ottawa, Ontario, May 12, 1999
www.privcom.gc.ca/speech/archive/02_05_a_990512_2_e.asp

House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities report, Privacy: Where Do We Draw The Line?, tabled in April 1997 (not available online)

Various Topics

A Guide for Canadians — Your Privacy Rights
Canada's Personal Information Protection and Electronic Documents Act
Office of the Privacy Commissioner of Canada
http://www.privcom.gc.ca/information/02_05_d_08_e.pdf

A Guide for Businesses and Organizations
Your Privacy Responsibilities
Canada's Personal Information Protection and Electronic Documents Act
Office of the Privacy Commissioner of Canada
http://www.privcom.gc.ca/information/guide_e.pdf

Human Rights in an Information Age: A Philosophical Analysis
Gregory J. Walters, University of Toronto Press, Toronto, Canada, 2001

Privacy Handbook for Canadians: Your Rights and Remedies
Brian Edy and the Alberta Civil Liberties Research Centre

Resource Guide

Contacts

Federal

The Privacy Commissioner of Canada

112 Kent Street, Ottawa, ON K1A 1H3
Tel.: 1 (613) 995-1376
Fax 1(613) 947-6850
E-mail: info@privcom.gc.ca.
www.privcom.gc.ca
1-800-282-1376

Treasury Board of Canada Secretariat
Corporate Communications

L'Esplanade Laurier, 10th Floor, West Tower
300 Laurier Avenue West
Ottawa, Canada K1A OR5
Tel: (613) 995-2855
Fax: (613) 996-0518
E-mail: services-publications@tbs-sct.gc.ca
www.tbs-sct.gc.ca

Oversee guidelines related to Federal PKI and privacy impact assessments.

Legislation Available Online

The Privacy Act

http://www.privcom.gc.ca/legislation/02_07_01_e.asp
The Privacy Act took effect on July 1, 1983

The Personal Information Protection and Electronic Documents Act (PIPEDA)

http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html
Part One of PIPEDA took effect as of January 1, 2001 and Part Two will come into effect on January 1, 2004.

PIPEDA Regulations

http://www.privcom.gc.ca/legislation/02_06_01_02_e.asp

Statistics Act

http://lois.justice.gc.ca/en/S-19/

Provincial and Territorial

Privacy Laws, Oversight Offices and Government Organizations

Alberta

Laws: Freedom of Information and Protection of Privacy Act
Health Information Act (came into force April 25, 2001)

Oversight: Frank Work
Information and Privacy Commissioner of Alberta
410, 9925 - 109 Street, Edmonton, Alberta T5K 2J8
Phone: (780) 422-6860

Fax: (780) 422-5682
Email: ipcab@planet.eon.net
Web Site: http://www.oipc.ab.ca/home/

Government Agencies Responsible:

Freedom of Information and Protection of Privacy Act
Information Management, Access and Privacy Division
Alberta Government Services
16th Floor, 10155 - 102 Street
Edmonton, Alberta, Canada T5J 4L4
Office Phone: (780) 422-2657
Help Desk Phone: (780) 427-5848
Fax: (780) 427-1120
Email: foiphelpdesk@gov.ab.ca
Web Site: http://www3.gov.ab.ca/foip/

Health Information Act
Alberta Health and Wellness
Email: inquiries (AHINFORM@health.gov.ab.ca)
Web Site: http://www.health.gov.ab.ca/

British Columbia

Law: Freedom of Information and Protection of Privacy Act

Oversight: David Loukidelis
Information and Privacy Commissioner for British Columbia
4-1675 Douglas Street
Victoria, British Columbia V8V 1X4
Phone: (250) 387-5629
Toll-free: 1 (800) 663-7867 (free within B.C.)
Fax: (250) 387-1696
Email: info@oipcbc.org
Web Site: http://www.oipcbc.org/

Government Agency Responsible:

Corporate Privacy and Information Access Branch
Information, Science and Technology Agency
Government of British Columbia
Victoria, British Columbia
Phone: (604) 660-2421
Email: EnquiryBC@gems3.gov.bc.ca
Web Site: http://www.mser.gov.bc.ca/FOI_POP/

Manitoba

Laws: Freedom of Information and Protection of Privacy Act
Personal Health Information Act

Oversight: Barry Tuckett, Ombudsman
Office of the Ombudsman
750 - 500 Portage Avenue
Winnipeg, Manitoba R3C 3X1
Phone: (204) 982-9130
Toll-free: 1 (800) 665-0531

Fax: (204) 942-7803
Email: ombusma@ombudsman.mb.ca
Web Site: http:/www.ombudsman.mb.ca/

Government Agency Responsible:
Freedom of Information and Protection of Privacy Act
Minister of Culture, Heritage and Tourism
Information Resources Division
3 - 200 Vaughan Street
Winnipeg, Manitoba R3C 1T5
Phone: 204-945-2142
Fax: 204-948-2008
Email: govrecs@gov.mb.ca
Web Site: http:/www.gov.mb.ca/chc/fippa/index.html

New Brunswick

Laws: Protection of Personal Information Act

Oversight: Ellen King, Ombudsman
Province of New Brunswick
767 Brunswick Street
P.O. Box 6000
Fredericton, New Brunswick E3B 5H1
Phone: (506) 453-2789
Toll-free: 1 (800) 561-4021 (free within N.B.)
Fax: (506) 453-5599
Email: nbombud@gnb.ca

Newfoundland

Laws: Freedom of Information Act
Privacy Act

Oversight: Chris Curran, Director of Legal Services
Department of Justice of Newfoundland
Confederation Building
P.O. BOX 8700
St. John’s, Newfoundland A1B 4J6
Phone: (709) 729-2893
Fax: (709) 729-2129
Email: chrisc@mail.gov.nf.ca
Web Site: http://www.gov.nf.ca/just/

Northwest Territories

Law: Access to Information and Protection of Privacy Act

Oversight: Elaine Keenan Bengts
Information and Privacy Commissioner of the Northwest Territories
5018, 47th street
Yellowknife, Northwest Territories X1A 2N2
Phone: (867) 669-0976
Fax: (867) 920-2511
Email: atippcomm@theedge.ca

Nova Scotia

Law: Freedom of Information and Protection of Privacy Act

Oversight: Darce Fardy
Freedom of Information and Privacy Review Officer
Freedom of Information and Privacy Review Office
P.O. Box 181
Halifax, Nova Scotia B3J 2M4
Phone: (902) 424-4684
Fax: (902) 424-8303
Email: uarb.dfardy@gov.ns.ca
Web Site: http://www.gov.ns.ca/foiro/

Government Agency Responsible:
Nova Scotia Department of Justice
General Information
5151 Terminal Road
P.O. Box 7
Halifax, Nova Scotia B3J 2L6
Phone: (902) 424-4030
Web Site: http://www.gov.ns.ca/just/foi/foisvcs.htm

Nunavut

Law: Access to Information and Protection of Privacy Act

Oversight: Elaine Keenan Bengts
Information and Privacy Commissioner of Nunavut
5018, 47th street
Yellowknife, Northwest Territories X1A 2N2
Phone: (867) 669-0976
Fax: (867) 920-2511
Email: atippcomm@theedge.ca

Ontario

Laws: Freedom of Information and Protection of Privacy Act
Municipal Freedom of Information and Protection of Privacy Act

Oversight: Ann Cavoukian
Information and Privacy Commissioner of Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario M5S 2V1
Phone: (416) 326-3333
Toll-free: 1 (800) 387-0073 (free within Ontario)
Fax: (416) 325-9195
Email: info@ipc.on.ca
Web Site: http://www.ipc.on.ca/

Government Agencies Responsible:
Freedom of Information and Protection of Privacy Act
Municipal Freedom of Information and Protection of Privacy Act
Information and Privacy Office
Office of the Corporate Chief Strategist
Management Board Secretariat
8th Floor, Ferguson Block

77 Wellesley Street West
Toronto, Ontario M7A 1N3
Phone: (416) 327-2187
Fax: (416) 327-2190
Email: web.foi@mbs.gov.on.ca
Web Site: http://www.gov.on.ca/mbs/english/fip

Prince Edward Island

Law: Freedom of Information and Protection of Privacy Act

Oversight: Karen A. Rose
Information and Privacy Commissioner of Prince Edward Island
J. Angus MacLean Building
180 Richmond Street
P.O. Box 2000
Charlottetown, Prince Edward Island
C1A 7N8
Telephone: (902) 368-4099
Fax: (902) 368-5947
Email: karose@gov.pe.ca
Web Site: http://www.gov.pe.ca/

Government Agency Responsible:
Office of the Attorney General
Fourth Floor, Shaw Building
95 Rochford Street
P.O. Box 2000
Charlottetown, P.E.I. C1A 7N8
Phone: (902) 368-4550
Fax: (902) 368-5283
Web Site: http://www.gov.pe.ca/foipp/index.php3

Quebec

Laws: Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information
Act Respecting the Protection of Personal Information in the Private Sector

Oversight: Jennifer Stoddart, Chair
La Commission d'accá l'information du Québec
575, rue St. Amable
Bureau 1.10
Québec, Québec G1R 2G4
Phone: (418) 528-7741
Fax: (418) 529-3102
Toll-free: 1 (888) 528-7741 (free within Quebec)
Email: Cai.Communications@cai.gouv.qc.ca
Web Site: http://www.cai.gouv.qc.ca/

Government Agency Responsible:
Ministère des relations avec les citoyens et de l'immigration
Director of Communications
Gérald-Godin Building
360, rue McGill, 2nd Floor
Montréal, Québec H2Y 2E9

Phone: (514) 873-4546
Fax: (514) 873-7349
Email: direction.communications@mrci.gouv.qc.ca

Saskatchewan

Laws: Freedom of Information and Protection of Privacy Act
Local Freedom of Information and Protection of Privacy Act
Health Information Protection Act (not yet in force)

Oversight: Richard Rendek, Q.C.
A/Information and Privacy Commissioner of Saskatchewan
208 - 2208 Scarth Street
Regina, Saskatchewan S4P 2J6
Phone: (306) 787-8350
Fax: (306) 757-8138
Web Site: http://www.legassembly.sk.ca/officers/informat.htm

Government Agencies Responsible:

Freedom of Information and Protection of Privacy Act
Saskatchewan Justice
11th Floor, 1874 Scarth Street
Regina, Saskatchewan S4P 3V7
Phone: (306) 787-5473
Fax: (306) 787-5830
Web Site: http://www.saskjustice.gov.sk.ca/legislation/summaries/freedomofinfoact.shtml

Health Information Protection Act

Saskatchewan Health
Email: webmaster@health.gov.sk.ca
Web Site: http://www.health.gov.sk.ca/ph_br_health_leg_hipamain.html

Yukon

Law: Access to Information and Protection of Privacy Act

Oversight: Hank Moorlag
Ombudsman and Information and Privacy Commissioner of the Yukon
211 Main Street, Suite 200
P.O. Box 2703
Whitehorse, Yukon Territory Y1A 2C6
Phone: (867) 667-8468
Fax: (867) 667-8469
Email: email.ombudsman@ombudsman.yk.ca
Web Site: http://www.ombudsman.yk.ca/

Government Agency Responsible:

ATIPP Office
Information & Communications Technology Division
Department of Infrastructure
Government of Yukon
2071-2nd Avenue
Box 2703
Whitehorse Yukon Y1A 2C6
Phone: (867) 393-7048
Fax: (867) 393-6916

Email: atipp@gov.yk.ca
Web site: http://www.atipp.gov.yk.ca/

Other Federal Offices

Canadian Security Intelligence Service (CSIS)
P.O.Box 9732
Postal Station T
Ottawa, Ontario K1G 4G4
(613) 993-9620
www.csis-scrs.gc.ca

Federal Department of Justice
The Honourable Martin Cauchon
Minister of Justice and Attorney General of Canada
284 Wellington Street
Ottawa, Ontario
K1A 0H8

Communications Branch
Tel: (613) 957-4222
TDD/TTY: (613) 992-4556
Fax: (613) 954-0811
Media Relations tel: (613) 957-4207
canada.justice.gc.ca/en/index.html

Health Canada
A.L. 0900C2
Ottawa, Ontario, K1A 0K9
Canada
Tel: (613) 957-2991
Fax: (613) 941-5366
Email: info@hc-sc.gc.ca
www.hc-sc.gc.ca

Office of Health and the Information Highway (OHIH)
Jeanne Mance Building, 4th floor
Postal Locator 1904
Ottawa, Ontario K1A 0K9
Tel: (613) 957-0706
Fax: (613) 952-3226
Email: ohih-bsi@hc-sc.gc.ca
www.hc-sc.gc.ca/ohih-bsi

Human Resources Development Canada (HRDC)
www.hrdc-drhc.gc.ca

To obtain HRDC publications:

Publications Centre
Human Resources Development Canada
140 Promenade du Portage, Phase IV
Hull, Quebec K1A 0J9
Fax: (819) 953-7260
pub@hrdc-drhc.gc.ca

Royal Canadian Mounted Police
RCMP Headquarters
1200 Vanier Parkway
Ottawa, ON K1A 0R2
www.rcmp-grc.gc.ca

Supreme Court of Canada
301 Wellington St.
Ottawa, Ontario
K1A 0J1
Tel: (613) 995-4330
Fax: (613) 996-3063
Email: reception@scc-csc.gc.ca
www.scc-csc.gc.ca/

Social Insurance Registration
P.O. Box 7000
Bathurst, New Brunswick
E2A 4T1

Legislated uses of the SIN (or legislation that regulates its use):

1. Budget Implementation Act (Canada Education Savings Grants)
2. Canada Elections Act
3. Canada Labour Standards Regulations (Canada Labour Code)
4. Canada Pension Plan Regulations (Canada Pension Plan)
5. Canada Student Financial Assistance Act
6. Canada Student Loans Regulations (Canada Student Loans Act)
7. Canadian Wheat Board Act
8. Employment Insurance Act
9. Excise Tax Act (Part IX)
10. Garnishment Regulations (Family Orders and Agreements Enforcement Assistance Act)
11. Farm Income Protection Act
12. Gasoline and Aviation Gasoline Excise Tax Application Regulations (Excise Tax Act)
13. Income Tax Act
14. Labour Adjustment Benefits Act
15. Old Age Security Regulations (Old Age Security Act)
16. Race Track Supervision Regulations (Criminal Code)
17. Tax Rebate Discounting Regulations (Tax Rebate Discounting Act)
18. Veterans Allowance Regulations (War Veterans Allowance Act)

Programs Authorized to use the SIN:

1. Immigration Adjustment Assistance Program;
2. Income and Health Care Programs;
3. Income Tax Appeals and Adverse Decisions;
4. Labour Adjustment Review Board;
5. National Dose Registry for Occupational Exposures to Radiation;
6. Rural and Native Housing Program;
7. Social Assistance and Economic Development Program

Organizations Active in Privacy (not exhaustive)

The Canadian Civil Liberties Association
www.ccla.org

Access to Justice Network
www.acjnet.org/

Alberta Civil Liberties Research Centre
www.aclrc.com

Association de la Sécurité de l'Information de la Région de Québec (ASIRQ)
www.asirq.qc.ca/fr/index.html

BC Civil Liberties Association
www.bccla.org

BC Freedom of Information and Privacy Association
http://fipa.bc.ca/

The Telehealth Ethics Observatory, Clinical Research Institute of Montreal
www.ircm.qc.ca/bioethique/english/telehealth/

Citizens Council on Health Care
http://www.cchconline.org/

Canadian Human Rights Commission
www.chrc-ccdp.ca

Canadian Medical Association
http://www.cma.ca

Canadian Trade Unions on the Net
www.politicalresources.net/canada/ca-unions.htm

Centre for Innovation Law and Policy, University of Toronto
www.innovationlaw.org

Commonwealth Centre for e-Governance
www.electronicgov.net

Democracy Watch
www.dwatch.ca

Electronic Frontier Canada
http://insight.mcmaster.ca/org/efc/efc.html

Fédéation informatique du Québec (FIQ)
www.fiq.qc.ca

Ligue des droits et libertes
www.liguedesdroitsqc.org

Manitoba Association of Rights and Liberties
www.winnipeg.freenet.mb.ca/marl/marl_hm.html (page under construction)

PEN Canada
www.web.net/~pencan/

The Public Interest Advocacy Centre
www.piac.ca

Coalition pour la surveillance internationale des libertés civiles (CSILC)
Contact: Roch Tassé Guy Caron
Coordonnateur Relations avec les médias
Groupe de surveillance international des libertés civiles Conseil des Canadiens
(613) 241-5298 (613) 233-2773 poste 234
rocht@iclmg.ca gcaron@canadians.ca