Ombudsman Manitoba

Special Report

A PRIVACY SNAPSHOT

Taken September 1999

Access and Privacy
November 1999

Ombudsman Manitoba

750 – 500 Portage Avenue
Winnipeg, Manitoba R3C 3X1
Telephone: (204) 982-9130
Toll Free in Manitoba:
1-800-665-0531
Fax: (204) 942-7803

500 av. Portage, Pièce 750
Winnipeg (MB) R3C 3X1
Téléphone: (204) 982-9130
Sans Frais au Manitoba: 1-800-665-0531
1-800-665-0531
Télécopieur: (204) 942-7803

To the Members of the Manitoba Legislature:

In view of the many recent unprecedented, complex and dynamic privacy issues touching the public, government and our office, this Special Report has been prepared as a "Snapshot" of today's privacy environment.

Under section 58(3) of *The Freedom of Information and Protection of Privacy Act* and section 37(3) of *The Personal Health Information Act*, the Provincial Ombudsman may, in the public interest, publish a Special Report relating to any matter within the scope of the powers and duties of the Ombudsman. Among these responsibilities is a duty to inform the public about these two enactments. As well, the Ombudsman's Office serves as an oversight function concerning the collection, use, disclosure and security of personal information and personal health information.

This Special Report is intended to contribute to a general awareness and public discussion of the privacy issues that confront us all daily.

B Tuckett

Barry Tuckett
Ombudsman

A PRIVACY SNAPSHOT
Taken September 1999

CONTENTS

A PRIVACY SNAPSHOT

Taken September 1999

INTRODUCTION

The Ombudsman's Office oversees the compliance of most provincial public sector organizations[1] and some private sector professionals[2] with privacy protection laws in Manitoba.[3] Since *The Freedom of Information and Protection of Privacy Act* and *The Personal Health Information Act* are recent enactments, we felt it would be useful to provide a sample of the complex debate about privacy rights, not just in Manitoba, but also nationally and internationally. We have called our overview a "Snapshot" because of the rapidly evolving character of privacy issues in the current information environment. Our portrayal of the *status quo* is likely to be overtaken even as we issue this snapshot.

It is a commonplace statement that national borders have fallen virtually before the onslaught of opportunities offered by electronic communications. Marshall McLuhan's "global village" seems to have become a reality. By the same token, privacy has become an issue transcending provincial and national borders. Hardly a day goes by without new information, debate, and concerns about personal privacy appearing in the news media and on the Internet. Sometimes it is difficult to distinguish between authoritative information and what may be considered sensationalized speculation or even scaremongering. Nevertheless, there is no doubt that information privacy in a global communication context has become a major public policy issue encompassing much more than the Internet.

The spectre of "Big Brother" is conjured frequently by authors attempting to portray the potential effect of widespread misuse of electronic communications. In 1998, the Canadian Broadcasting Corporation aired a two-part televised series on modern surveillance activities entitled "No Place to Hide". In recognition of two major segments of society holding vast amounts of personal information about us, the series characterized the public sector as "Big Brother" and the private sector as "Little Brother". *The Winnipeg Free Press* carried an editorial on July 27, 1998, which noted that "The erosion of privacy, in fact, is one of the most worrying features of the revolution in electronic communications that are occurring an ever-faster pace." *The Globe and Mail* observed on April 16, 1998: "As usual, we've embraced the technology before we've understood its effects.... Privacy is becoming a number-one concern for Canadians in the electronic age." A commentary in *The Winnipeg Sun* suggested that "Our legislators may need to look at stronger privacy legislation to shield people from 'Big Brother' style abuse... by the usual public and private busybodies."[4]

With the accelerating advances in computing and electronic communications, personal information has become a focus of intense interest by many organizations and individuals for a variety of purposes ranging from commerce to research, from service to the public to public safety, and from personal to national security. It has been characterized as a commodity and the protection of it as a human right. While the proper use of personal information can be benign or even beneficial, the abuse of it can lead to consequences ranging from the merely irritating to the terrifying. If there is any message to be drawn from our "Snapshot", it is simply that the public needs to be aware of privacy issues and competing interests so that individuals can make informed and balanced choices about the collection, use, and disclosure of their personal information whether by public or private sector entities.

We have included endnotes for this snapshot in order to provide information sources and Internet links for those who may wish to explore privacy issues in an electronic environment. Be prudent about accepting too many "cookies".

WHAT IS PRIVACY?

The answer varies, because the concept of "privacy" may encompass a number of dimensions:

- ***privacy of the person.*** *This is concerned with the integrity of the individual's body. Issues include compulsory immunization, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilization;*
- ***privacy of personal behaviour.*** *This relates to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places;*
- ***privacy of personal communications.*** *Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organizations; and,*
- ***privacy of personal data.*** *Individuals claim that data about themselves should not be automatically available to other individuals and organizations, and that, even where data is held by another party, the individual must be able to exercise a substantial degree of control over that data and its use.*[5]

In Manitoba, *The Freedom of Information and Protection of Privacy Act* (FIPPA) and *The Personal Health Information Act* (PHIA) protect the privacy of personal information and personal health information. While other privacy interests may indirectly benefit from the legislation, the primary purpose of both laws is the protection of *data privacy* within the province. Taken together, these Acts provide a legal right of privacy for personal information held by public bodies and personal health information held by a public trustee, including public bodies, and a personal health information manager. These access and privacy rights do not extend into the private sector with the notable exception of important areas defined under PHIA, which nevertheless do not include some significant "users" of personal health information such as private employers and insurance companies.

Both Manitoba statutes are based on principles of Fair Information Practice developed by the Organisation for Economic Co-operation and Development (OECD) in 1980.[6] According to these principles, an organization is obligated to:

- identify the reason for collecting, using and disclosing personal information;
- obtain consent before collecting, using and disclosing personal information;
- collect the minimum amount of information needed to accomplish its purpose;
- use and disclose personal information only for the same reasons it was collected (unless consent is obtained);
- ensure the accuracy of personal information;
- provide individuals with access to their own information and allow them to make corrections if needed;
- keep personal information only for as long as it is needed;
- ensure the security of personal information; and,
- provide a complaint process and an independent review process.[7]

When information moves beyond provincial borders, the Manitoba legislation loses its jurisdiction and its legal ability to protect the privacy of the information. Data held by much of the federal public sector is, however, covered under the 1982 federal *Privacy Act*.

Other privacy interests may receive limited protection under the Canadian *Charter of Rights and Freedoms* (the *Charter*). It is important to understand that Canadians do not have an inherent or codified "right to privacy".

Privacy of the person is preserved, to a degree, by s.7 of the *Charter*.[8] This provision states that everyone has the right to life, liberty and security of the person, and cannot be denied this right except in accordance with the principles of fundamental justice (similar to "due process"). The privacy protection is essentially limited to circumstances where an individual is detained or incarcerated by the government. While the person may decline requests for bodily fluids, tissue samples, and medical procedures while under the "control" of the state, the state may nevertheless overcome the individual's lack of consent if it is in the public interest of "a free and democratic society".[9]

Communication and data privacy may be preserved under s.8 of the *Charter*, depending on the particular circumstances of the case. According to this provision, everyone has the right to be secure against unreasonable search and seizure. A major limitation to the privacy protection is that the "search and seizure" must be unreasonable to be prohibited. Court cases have determined that the right to privacy only exists in places and circumstances where people have a "reasonable expectation of privacy".[10] Whether or not someone may reasonably expect privacy has been based on factors such as possession or control or ownership of the place searched, ability to regulate access to the place searched, and the objective reasonableness of the privacy expectation. Therefore, intercepting communications and conducting surveillance would likely not be considered "unreasonable" in public places.

Another limitation of the law is that individuals are protected against intrusions by "agents of the state", but not surveillance by the private sector. Therefore, while the state is generally not allowed to intercept telephone calls without a warrant, an employer may routinely read employees' e-mail or monitor employees' activities over closed circuit TV cameras.

Efforts to protect privacy in Manitoba have been directed toward ensuring the privacy of *personal information* held by the public sector, rather than directly preserving the privacy of individuals. It is expected that the ability to control who has access to personal information will ultimately provide a measure of personal privacy. Data privacy laws are intended to place control firmly in the hands of the individual the information is about:

> *Remember your personal information belongs to you, no one else. Governments, banks, and other organizations who need your information often forget that they act only as the custodians of the information you entrust to them, and which they are responsible for safekeeping. They do not own it.*[11]

Manitoba's emphasis on data privacy protection is consistent with the approach taken nationally,[12] as well as internationally[13] in the European Union, Australia, New Zealand, Hong Kong and the United States.[14]

Some aspects of the provincial legislation have drawn international attention.[15] Manitoba has been recognized for its efforts to regulate the collection, use and disclosure of personal *health* information. *The Personal Health Information Act* is not only the first legislation in Canada to

regulate the privacy of personal health information – it is also the first statute to explicitly protect health information held by health professionals in the private sector.

WHY IS PRIVACY IMPORTANT?

Surveys and studies reveal clearly that Canadians value their privacy. The Canadian Privacy Survey in 1992 found that most Canadians were moderately to extremely concerned about personal privacy (92%).[16] A 1994 Equifax Canada survey revealed that the majority of Canadians (76%) were concerned about privacy, and believed they had lost control over the dissemination and use of personal information about them (70%).[17] A 1995 study by the Public Interest Advocacy Centre (PIAC) confirmed that Canadians want to control their personal information:

> *Canadians want to be informed about collection processes and about the uses to which their personal information may be put (95%). They insist that their permission be sought and given before any such information is passed on to another organization (94%).*[18]

This study also found that privacy perceptions reflected socio-economic variables:

> *The most noticeable cleavage is along class lines. Opinions about invasiveness and justification [of specific information practices] often vary with income and education, but also with age. For instance, higher-income [survey] respondents will be more concerned about charities making uninvited solicitation calls and selling their donor lists, whereas lower-income respondents are more concerned about banks requiring their employment status in order to simply open a bank account or about Revenue Canada and Employment Canada sharing information to prevent fraud.*[19]

What have you got to hide?

Despite the importance of privacy, it is sometimes described in terms that arouse suspicion – the right to be anonymous, secretive or unseen. These values seem to be important only if a person has something (presumably immoral or illegal) to hide. This suspicion can cause a subtle shift when considering information privacy issues. Rather than asking organizations to justify the collection of information, individuals are asked to justify their refusal to provide information.

But privacy preserves more than secrets. In addition to the "right to retreat from the world", privacy confers a "right to control information about oneself, even after divulging it to others":

> *Privacy, as defined here, allows individuals to choose when to withdraw and when to participate. People must be able to seek solitude and isolation from others to develop a sense of themselves apart from others. Developing one's unique identity is critical to a person's ability to form his or her own thoughts and opinions and to establish intimate connections with others. A society that preserves privacy for its people is one that acknowledges the individual's interest in maintaining control over his or her life. One aspect of this control is being able to determine the presentation of one's self, or various pieces of one's self, to others. A person who is unable to retreat feels constantly watched, dehumanised, and powerless to make fundamental decisions affecting his or her own life.*[20]

According to this view, privacy is fundamental to other constitutional and democratic rights, including freedom of conscience, freedom of thought, freedom of expression, the right to vote, and the rights to liberty and security of the person. Without the privacy of a secret ballot, for example, citizens could not fully exercise their right to vote. Therefore, we can conclude that privacy is important because it provides positive social benefit.

SHOULD PRIVACY BE A HUMAN RIGHT?

Privacy International's[21] 1998 report *Privacy and Human Rights: an international survey of privacy laws and practices* states:

> *Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age.*[22]

Taking a broad definition of the elements of personal privacy,[23] the report points out that Canada has no explicit right to privacy. If privacy were defined as a fundamental human right under the federal *Charter of Rights and Freedoms*, it would extend beyond the basic protection of data and information to encompass privacy of the person and that person's behaviour.

Some advocates argue that privacy should be entrenched as a charter right and include physical, bodily and psychological integrity; freedom from surveillance; and privacy of personal space. In this view, people should be able to choose how they wish to participate in the world.[24] Among the benefits would be recognition that governments and businesses do not have an inherent right to conduct surveillance or create "consumer" profiles of people. It is argued that, unless privacy is explicitly recognized as a right, it risks becoming just another commodity that individuals are expected to exchange for goods and services.

If privacy were a *Charter* right, it would be balanced against other human rights, rather than against commercial interests. It would be viewed as a "public good" rather than as part of the "economic infrastructure".[25] It has been argued that even though privacy is not a constitutional right in Canada, we should nevertheless approach policy decisions as if it were:

> *If we approach privacy issues from a human rights perspective, the principles and solutions we arrive at will be rights-affirming, people-based, humanitarian ones. ...[I]f we adopt a market-based or economic approach, the solutions will reflect a different philosophy, one that puts profit margins and efficiency before people, and may not first and foremost serve the common good.*[26]

In short, the argument is that if privacy were entrenched as a human right in Canada, it would provide a baseline for all citizens and residents in their interactions, whether with public or private-sector entities. Nevertheless, Canada and most of its provinces and territories do have information access and privacy legislation dealing with personal information held by public bodies. Quebec is distinguished by having a law that also regulates personal information held by private sector businesses operating in that province.

ARE WE LOSING CONTROL OVER PERSONAL INFORMATION?

In the public sector, obtaining goods or services generally requires a person to provide some level of personal information. The amount or sensitivity of intimate personal information collected is often proportional to the type of service required. Users of medical and social assistance services rank at the highest levels of demand for personal information and frequently represent the most vulnerable segments of society. In short, those in greatest need or at lower income levels often provide greater amounts of information to enable or justify provision of goods and services from the public sector.

This mandatory collection of personal information is subject to information access and privacy laws in Manitoba to control and manage the collection, use and disclosure of personal information. These Acts were passed in recognition of the fact the electronic recordkeeping capabilities and new communication technologies can lead to improved provision of better services, but also put vast volumes of electronic information at greater risk of misuse by inappropriate data sharing. The personal information privacy components of the Acts were developed in the context of increased demand for such information in both the public and private sectors of society.

Information technology advances are causing custodians of public records to re-examine the purposes and uses of traditionally accessible records held, for example, in relation to personal information-intensive public registries such as real estate, personal property, assessments, and driver and vehicle licensing registries. Some of these registries have been available for public scrutiny on a case-by-case or limited-number basis over the years. Electronic technologies have enabled access to and manipulation of the information on a scale never envisaged when the registry systems were developed and sanctioned by law or policy. The disclosure of personal information in these types of records on a bulk or volume basis is specifically controlled under Manitoba access and privacy laws, as is the linking and matching of personal information contained in public registries or other collections of personal information. This control does not challenge traditional public access to such public records, but it does control the use and disclosure of personal information by public bodies other than the custodian of the information and by private organizations.

In the private sector, as in the public, significant opportunities are being envisaged, explored, and developed to improve the provision of goods and services to the public through the use of electronic technologies. Collection of personal information in the course of trade and commerce has become a distinct component of many businesses, and the sharing or marketing of this information is becoming ever more commonplace. Privacy advocates argue that the collection, use and disclosure of personal information in the private sector should be subject to Fair Information Practices to protect the privacy of individuals. A number of companies *do* treat this information securely and ethically, but the potential and actual misuse of personal information has become a focus of national and international debate which revolves about state or self-regulation of the collection, use, and disclosure of personal information.

Some businesses ask people to, in effect, exchange varying amounts of their personal information for bonus points, discounts and "free" merchandise. While individuals may receive something for their loss of privacy, is it a fair exchange? It has been argued that individuals are not in a position to bargain fairly. They are often unaware of any or all the uses to which their information will be put. There are few, if any, effective laws in place that provide recourse to consumers for breaches of privacy in the commercial sector. As well, most individuals cannot

truly "negotiate" the price of their privacy – it is a "take it or leave it" proposition. This becomes less benign when it is understood that the collection of personal information is largely unnecessary to the commercial transaction – the consumer simply wishes to obtain an article of clothing, but the retailer may want payment for the value of the item *and* personal information.[27]

Despite the high levels of concern identified in public opinion surveys, an individual's control over his or her own personal information appears to be slipping. It seems that an increasing number of unintended privacy breaches are being reported in the media. Perhaps the largest exposure of Canadian data occurred in January 1999, when the personal information of as many as 50,000 Canadian participants in Air Miles was revealed.[28] Eighty-two categories of information could be viewed, including name, address, telephone number, e-mail address, types of credit cards held, and number of vehicles owned.

In April 1999, a rash of unintended privacy breaches were reported in the United States, including:

- 1,800 email addresses accidentally revealed to other customers of AT&T;
- 24,000 email addresses inadvertently sent to potential customers of Nissan;[29]
- 1,500 email addresses mistakenly sent to customers of Seagate Software,[30] and names, addresses and full credit-card numbers of customers for at least 100 small business sites on the Internet.[31]

Perhaps more troubling are privacy controversies that arise from the *intentional* collection, use and disclosure of personal information.

SURVEILLANCE

"Surveillance" involves monitoring people and locations, as well as intercepting communications.

The amount of visual monitoring taking place through the proliferation of closed circuit television and video surveillance cameras is increasing. In the United Kingdom, for example, it is estimated that there are currently 1,000,000 video cameras conducting surveillance in public spaces.[32] This surveillance is credited with significant reductions in criminal activity. Privacy advocates will point out that although the serious terrorist threat in Britain was a prime motive in developing this system, questions can be raised about the real overall effects of video surveillance. Does criminal activity simply move from the areas under surveillance to new locations, setting off a never-ending installation of more and more surveillance systems that scrutinize everyone indiscriminately?

Surveillance cameras can be manipulated from a remote site and be equipped with "night vision". They can "follow" and even identify people as they move through public and private spaces. With the advent of digital cameras and digital camcorders, these images can be readily used on personal computers and transmitted electronically. One recent article predicted that the sharing of video-clips would soon become as common as e-mail.[33] As it becomes easier to collect and store digital images, the likelihood that these images will be used to reconstruct a person's daily movements and activities also increases.

ENFOPOL is "a sniper's bullet in the head of privacy."
Ian Brown
Policy Director
Privacy International

Surveillance networks are becoming transnational. In particular, two global networks have drawn media attention over the past year. ENFOPOL is an "eavesdropping" system that will allow authorities to intercept any mobile phone calls, Internet communications, fax transmissions and pager messages in Europe, regardless of the country of origin. The strategy calls for communications devices that will support wiretapping, encryption codes that can be broken, and a "subject tagging" system that can track people geographically:

> *...[T]he tagging system will create a data processing and transmission network that involves not only the names, addresses and phone numbers of targets and associates, but email addresses, credit card details, PINs and passwords.*
>
> *But the proposal has infuriated civil liberties and Internet rights organizations. Ian Brown, technology policy director of Privacy International, calls it a 'sniper's bullet in the heart of privacy'.*[34]

Another global surveillance system which has recently attracted attention is ECHELON. It targets all the key Intelsat satellites used to convey the majority of the world's satellite transmissions, including phone calls, Internet, email, faxes and telexes. As reported in a working document to the European Parliament:

> *ECHELON is designed for primarily non-military targets: governments, organisations and businesses in virtually every country. The ECHELON system works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence aids like Memex to find key words. Five nations share the results with the US as the senior partner under the UKUSA agreement of 1948; Britain, Canada, New Zealand and Australia are very much acting as subordinate information servicers.*[35]

It is not just wireless communications that are being intercepted. In preparing for a civil trial against a company in the United States, attorneys made a routine request for any recordings that would be relevant to the case. Company officials admitted that conversations had been surreptitiously recorded within a five-foot radius of microphones lodged in employees' computers:

> *It turns out that virtually every computer system purchased after March 1996 contains a microphone, and that the IT departments at Polar and other companies had routinely been using special sound-activated software to record and collect conversations.*[36]

The author claims that any individual with a computer purchased after March 1996 could be under audio surveillance without even knowing it.

DATAVEILLANCE

Dataveillance, a term coined by privacy advocate Roger Clarke,[37] involves the use of recorded information about people and their activities. It can target individuals for special investigations

or expose broad segments of the population to scrutiny. Whether the goal is to monitor transactions on a routine basis or conduct a single data-matching project, dataveillance requires the use of *identifiers*.

Dataveillance requires identifiers to connect bits of information to an individual. The proliferation of identifiers has attracted the attention of privacy and consumer groups in the United States. In February 1999, they instigated a boycott and filed a complaint with the Federal Trade Commission against Intel.[38] At issue was the unique identifier that was built into every Pentium III, Pentium II and Celeron computer chip. Privacy advocates argued that the identifier would make it easier to track computer users and their activities as they "surfed" the Internet.

The company claimed that the identifier was intended to enhance security and encourage online shopping ("e-commerce"). Vendors could authenticate the identity of a purchaser by matching the unique identifier with the person's name and credit card number. Credit card fraud would be reduced over the Internet, it was assumed, because an impersonator would require a person's name, credit card *and* actual computer.

While the Pentium III is still on the market, and still has the capability to electronically communicate its unique identifier, the privacy groups have been successful in persuading Intel to turn the identifier capability "off" before the computers are sold to the public. In other words, customers have been given the choice of whether to activate the identifier. Their complaint to the Federal Trade Commission has yet to be resolved.

A number of other software and hardware identifiers have been exposed. As with the Pentium III chip, the companies did not publicize the tracking capabilities of the following identifiers:

- Global unique identifier (capable of connecting a document with its author) in all Microsoft documents created using Microsoft Office 97; and
- Unique device identifiers (capable of connecting a device with its user) assigned to any network device by Sun Microsystems Jini software.

These identifiers enable data matching and linking. *Data matching* is a form of mass dataveillance that involves comparing records from different electronic databases. The purpose of the comparison is to find "matches" where there should be none (such as the receipt of social assistance and the receipt of employment insurance) or to detect "no matches" when there should be (such as evidence of corporation registration without corresponding evidence that the company filed income tax returns).

In an effort to increase efficiency and decrease costs, public sector agencies are using the technique of data matching more frequently. Since data matching endangers Fair Information Practices,[39] there have been attempts to impose reasonable and fair limits on these projects. At the federal level, there is a policy stipulating that all data-matching proposals, including a cost-benefit analysis, must be sent to the Federal Privacy Commissioner for assessment.[40] In Manitoba, public bodies must seek an opinion from the Privacy Assessment Review Committee (PARC) prior to linking databases.[41]

While the use of modern information technologies can contribute to the provision of better services, it should not be presumed that all data-matching proposals would result in public sector efficiencies. "Project Match", for example, was the first large-scale data-matching program carried out by the United States government. In 1977, the Department of Health, Education &

Welfare compared the records of those receiving Aid to Families with Dependent Children (social assistance) with the records of 3,000,000 persons employed by the federal government:

> *It identified 33,000 raw hits, later reduced to 7100, resulting in 638 internally investigated cases, of which 55 resulted in prosecution. ...[T]hese prosecutions resulted in only about 35 convictions, all for minor offences, with no custodial sentences and less than $10,000 in fines.*[42]

When the costs of the project (resources to create the records for the match, perform the comparison, investigate the findings and prosecute the cases) were taken into account, it was determined that the project was not cost-effective.

Research into data-matching programs in the United States, Canada, Australia and New Zealand concluded that of all the people whose data is examined during the matching process, only a very small proportion are eventually identified as meeting the project criteria:

> *Research conducted by the author shows that typically between 1% and 9% of records generate raw hits, and 0.1 – 2.0% survive the filtering process and reach the analysis stage. In the case of the Australian Department of Social Security's parallel matching scheme, the proportion of raw matches which have resulted in downward variations in benefits has been only about 0.5%, with 0.2% leading to debt recovery action in relation to overpayments.*[43]

The main reason for exercising caution, however, is the risk to privacy inherent in data-matching schemes. It frequently violates the principle that information collected for one purpose should not be used for another purpose without consent.

As an investigative tool, data matching is prone to error and inaccuracy. This results from attempts to match information from two databases that are not the same in content, structure, or design. In all likelihood, the databases have been compiled for different purposes, contain different types of information, and possess different degrees of reliability.

While exceptions to Fair Information Practices are made for the purpose of law enforcement, it should be stressed that data matching is often a "fishing expedition". Prior to the match, governments rarely have reason to believe that any particular person has committed any particular transgression. Therefore, matching may well violate the constitutional prohibition against unreasonable search and seizure. If every "match" is presumed to identify a guilty person, it could result in that person having to "prove" his or her innocence. This would subvert the traditional legal presumption that a person is considered innocent until proven guilty.

Data matching is a particularly invidious form of dataveillance because it promotes a narrow view of privacy, where matching is in the public interest and privacy is a personal concern. It can be difficult to argue for the paramountcy of privacy when the *social* benefits of data matching are usually weighed against *individual* costs to privacy. It has been argued that, if the social costs of monitoring and the social benefits of privacy were identified and considered, the emphasis would shift away from dataveillance.[44]

DATA NETWORKS

Increasingly, information collected from a variety of sources is stored in shared computer databases and is accessible through integrated networks. If the trend to data warehousing

continues, individuals will no longer have separate "files" with different organizations. Instead, an organization will have access to a temporary file that is assembled from all the bits of information that have been previously collected and stored.

This type of system can enhance privacy because information can be differentiated on a *need-to-know* basis. It is no longer necessary to provide access to the entire file. As well, computerized audit trails can be built into the system to ensure that only authorized access to information has occurred.

Networks can also pose risks to privacy. With unique identifiers, information from different sources can be linked whenever requested. This could eliminate the need for data-matching controls (legislated procedures or policies) and the oversight that accompanies those controls. But the greatest risk to privacy could arise from the loss of document "context". In a paper-based system, the document containing the information provides context for that information. For example, information may take on a different meaning depending on the document type (letter, affidavit, or questionnaire), source (investigator, individual, or advocate) and date. Without the appropriate context, bits of information become increasingly vulnerable to misconstruction and misinterpretation.

These trends point to declining control over our personal information, and lead to questions about the future of privacy.

THE END OF PRIVACY?

The convergence of computing and communication technologies means that the collection, storage, analysis and retrieval of information now occur on a vast scale. The capacity to process large volumes of information enables routine monitoring of everyday transactions and makes the "surveillance society" possible.[45]

Our understanding of the term "surveillance society" is influenced by George Orwell's *Nineteen Eight-four*, and its catch-phrase "Big Brother is watching you". In Orwell's society, the only institution to monitor individuals was the government; in contemporary society, however, many different organizations conduct surveillance. "Big brother" has been joined by his so-called "little brothers" in the private sector:

> *Just consider the amount of information already being collected as a matter of routine – any spending that involves a credit or bank debit card, most financial transactions, telephone calls, all dealings with national or local government. Supermarkets record every item being bought by customers who use discount cards. Mobile-phone companies are busy installing equipment that allows them to track the location of anyone who has a phone switched on. Electronic toll-booths and traffic-monitoring systems can record the movement of individual vehicles. Pioneered in Britain, closed-circuit TV cameras now scan increasingly large swathes of urban landscapes in other countries too. The trade in consumer information has hugely expanded in the past ten years. One single company, Acxiom Corporation in Conway, Arkansas, has a database combining public and consumer information that covers 95% of American households. Is there anyone left on the planet who does not know that their use of the Internet is being recorded by somebody, somewhere?*

Firms are as interested in their employees as in their customers. A 1997 survey by the American Management Association of 900 large companies found that nearly two-thirds admitted to some form of electronic surveillance of their own workers. Powerful new software makes it easy for bosses to monitor and record not only all telephone conversations, but every keystroke and e-mail message as well.[46]

The impact of all this monitoring on the future of privacy has been a source of controversy. Privacy advocates were incensed, for example, when the chief executive officer for Sun Microsystems baldly asserted: "You already have zero privacy – get over it."[47] Although extreme, this assertion forces us to consider whether the continuing erosion of control over personal information will lead to the "end of privacy".

"You already have zero privacy -- get over it."

Scott McNealy, CEO Sun Microsystems

We need to understand why privacy seems to be losing ground if we are going to forecast its future. One theory views the loss of privacy as the unintended, but inevitable, result of *technological change*. From this perspective, if computer programs have been developed with the capacity to construct detailed personal profiles, those profiles will be created and sold.

It is our observation, however, that most technology is inherently privacy-neutral. The positive or negative impact of technology depends on how it is used – and people are responsible for those decisions.

A good example is the use of encryption software. The software can "scramble" an e-mail message so that it cannot be read until it has been "unscrambled". If this type of software were widely used, communications privacy would be increased, but crime detection might be reduced. If, on the other hand, laws required that manufacturers provide "keys" to government and police (so they could read any encrypted communications without obtaining warrants), privacy would be reduced though public safety and national security could be enhanced.

Privacy protection is frequently a matter of balancing interests. The trick is that the real weights and values of the interests need to be determined, and assessments that involve personal information should be open and transparent to the public. Compromising the privacy of the many, or even of one person, may or may not be a price the public is willing to pay for certain invasive activities.

While information technology may be privacy-neutral, there must be privacy protection built-in at the systems technology design phase. The design should take into account the fact that systems have human as well as technological elements. Therefore, security safeguards, information audit provisions, and well understood written policies and practices must accompany the deployment of information technologies using personal information.

Data mining is considered by many privacy experts to be one of the most privacy-intrusive potential uses of electronic data banks where personal information is involved. Data-mining has been described as:

...a set of automated techniques used to extract buried or previously unknown pieces of information from large databases. Successful data mining makes it

possible to unearth patterns and relationships, and then use this 'new' information to make proactive knowledge-driven business decisions.[48]

Data-mining software can sift through immense volumes of information to create personal profiles. Uncontrolled use of this technique to track all consumer activities would significantly decrease privacy. A combination of legislation, policy, organizational commitment to privacy principles, and consumers insisting on protection of their personal information would, however, go a long way toward ensuring that the end of privacy will not be the inexorable consequence of technological change. These measures would protect privacy without eliminating the substantial public benefits of technological applications.

Some privacy experts are equally concerned that viewing privacy as a "bargaining chip" could gradually and seriously compromise it. From this perspective, the loss of privacy would be the incremental result of many separate decisions to "trade" privacy for security and services. The loss of privacy from the video surveillance of public spaces, for example, would be viewed as an exchange for increased public safety in those spaces. The loss of privacy from monitoring e-mail and computer use would be balanced by increased productivity. The loss of privacy from matching beneficiaries of one government program to another would be offset by increased protection from fraud.

In this view, the loss of privacy would be acceptable if it resulted from choice. Where elements of coercion appear, the bargain seems less appealing:

> *Unlike totalitarian states where citizens sacrifice their liberty to avoid persecution, network societies entice us into compliance and submission by offering us rewards and privileges. In exchange for credit and access – the modern equivalents of coloured glass beads – we offer up our personal privacy.*[49]

This "bargaining chip" perspective assumes that individuals can and do make informed choices about the degree of privacy they are willing to give up for a measure of security or in a commercial transaction. Making informed choices depends, however, on a number of factors including access to one's own personal information (to know what will be bargained away); knowledge of how the information will be used and who will see it (to appreciate the consequences of relinquishing information); and the ability to make a meaningful choice without coercion (to not suffer undue consequences for "opting-out" of an exchange).

Critics of this perspective maintain that even if people were able to assess the costs of trading away their privacy, there is still no guarantee that they will be in a fair bargaining position. Bargaining power depends, to a great extent, on the ability to walk away from an offer. In a real sense, where there are no real options available, the privacy risk is as great for those with resources as for those without; for instance, if all organizations demanded information as a price for service, consumers would have little or no bargaining power.[50]

It is probably premature to announce the death of privacy, but its healthy survival will require public affirmation of privacy as a positive and important social value.

How Can Privacy be Protected?

Privacy can be protected through legislation or self-regulation. Most public sectors in Canada now have privacy protection laws similar to those in Manitoba. The private sector has remained largely unregulated with the exception of businesses operating in Quebec[51] and health trustees

practicing in Manitoba.[52] To some, the 1996 publication of the *Model Code for the Protection of Personal Information* by the Canadian Standards Association (CSA), and its approval by the Standards Council of Canada, provided a major opportunity for private businesses to voluntarily balance their business needs for personal information with privacy rights. Development of the *Model Code* drew on significant experience and expertise from both the public and private sector. Some business sectors had, in effect, been treating personal information with respect and ethically for a number of years, and the *Code* simply confirmed or refined their existing practices. However, the rapid expansion of electronic technologies and opportunities for electronic commerce, seemed to outstrip the rate of implementation of commercial privacy practices based on the *Model Code* for the vast majority of businesses operating in Canada. In 1998, Canada introduced Bill C-54, the *Personal Information Protection and Electronic Documents Act*[53] confirming the shift in emphasis at the national level toward government regulation of the private sector.

Bill C-54, if enacted, would apply to any organization collecting, using or disclosing personal information in the course of inter-provincial or international activities or commercial activities. In essence, the law would make the application of Fair Information Practices mandatory for many parts of the business sector. This would be accomplished by including the ten principles from the CSA *Model Code*[54] as a schedule in Bill C-54. The ten principles include: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

There has been a significant amount of debate concerning whether legislation or industry self-regulation is more effective for protecting privacy in the commercial sector. In part, the fifteen-member European Union (EU) brought this debate to the forefront through its adoption of Directive 95/46/EC[55] in 1995. As summarized:

> *The e-commerce package aims to clarify the legal situation for consumers and companies who do business over the Internet, setting out rules in areas such as advertising, electronic contracts, liability, and professional standards.*[56]

The Directive stipulates that personal data cannot be transmitted to jurisdictions that do not provide adequate standards of privacy protection; the standards are based on Fair Information Practices. It was scheduled to come into effect by October 1998.

The Directive has had major implications for private sector data protection in other jurisdictions, since non-compliance may result in the suspension of data transfers and electronic commerce from European countries. Preferring industry self-regulation, the United States government and businesses have resisted the enactment of regulations.[57] Privacy legislation has been viewed as too costly and too interventionist. In a period of increased reliance on or preference for "one-to-one marketing", there is concern that restrictions on the ability of businesses to collect and sell customer profiles would affect the competitiveness of an enterprise. It is also feared that legislation would reduce or eliminate revenues, since profiles can be sold for as much as "...several hundred dollars for each name and address of a customer."[58]

In Canada, industry self-regulation has not been viewed with the same degree of optimism. A study in 1995 concluded the following:

> *Lastly, our survey shows that Canadians don't trust the private sector to self-regulate. When asked to choose among three options, only 7% of Canadians chose industry self-regulation over government regulation or greater public*

involvement in rule-making and enforcement of personal-information protection.[59]

Although the United States has been viewed as the most ardent proponent of self-regulation, there are increasingly vigorous calls for privacy regulation even in that country. Some of the pressure has resulted from the seeming failure of self-regulation.

A survey carried out by the Federal Trade Commission (FTC) in March 1998 found that only 14% of the 1400 sites reviewed in the study, informed visitors of their privacy protection practices.

90% of Internet privacy policies failed to comply with FTC standards

1999 Georgetown University Survey

A different study (with different methodology) in April 1999 found that while 66% of 364 sites had posted a privacy policy, and 94% of the top 100 sites had posted a privacy policy, only 10% of those policies actually complied with FTC guidelines.[60] This shows that even when web sites do post policies, 90% of those policies fail to meet the minimum standards set by the FTC.

Recent pressure has also been coming from an unexpected quarter – business executives and chief information officers. These leaders believe the EU Directive would impose a "level playing field" regarding consumer privacy:

> *The poll of 342 chief information officers (CIOs) and business executives was deployed March 29, 1999, at a CIO Perspectives conference in Phoenix. Poll results also show over two-thirds (73%) of respondents believe the United States should conform to Europe's stricter privacy standards.*[61]

One of the biggest hurdles faced by self-regulation proponents is the notion of "enforcement" – in effect, the compliance oversight role discharged in Canada by Commissioners or Ombudsmen. How can consumer protection be ensured without legislation? The private sector response has been certification programs administered by the Better Business Bureau (BBB) Online, the Online Privacy Alliance (OPA), and TRUSTe.

These programs have met with limited success. The BBB Online, for example, assesses only the applicant's current policies and practices for its web site, not its business in general. It has certified 14 Web sites and is assessing the applications for 240 other companies. Even with this relatively low number of approvals, the BBB Online is facing controversy:

> *Privacy advocates were astonished at the Better Business Bureau's decision last week to award a "privacy seal" to Equifax, a company with one of the worst records on privacy in the country.*
>
> *Based on information published by BBB about the seal program, we fear that BBB was constructed to use a similar tactic of evasion as that of another seal program, TRUSTe. In a recent incident with Microsoft, TRUSTe found that Microsoft breached consumer privacy but not their licensing requirements....That license draws a subtle distinction between the web site and the company. We consider such distinction deceptive and unfair, because consumers do not understand it and because it gives a false impression that their privacy will be protected by the company.*[62]

The TRUSTe certification program in the United States has been operating for more than a year. It assesses web sites to determine whether they conform to the TRUSTe conditions by adhering to baseline privacy and disclosure principles and submitting to enforcement by TRUSTe. Those sites that appear to conform are permitted to display a TRUSTe "trustmark".

Participation is voluntary, so coverage is not complete.[63] By the end of 1998, there were more than 300,000,000 web pages.[64] TRUSTe had licensed 600 sites by April 1999.[65] Although TRUSTe points out that 45 of the top 100 most trafficked Web sites are licensees (representing 35% of all U.S. Internet traffic), privacy protection is neither uniform nor comprehensive.

The ability of the TRUSTe system to provide independent oversight has been challenged. The program is funded by a number of large corporations, and is run by a board that includes executives from those corporations. This placed the program in a "delicate spot"[66] when Junkbusters, a privacy organization in the United States, filed a complaint against Microsoft with TRUSTe. Microsoft contributed $100,000 in funding, and has an executive on the board.

TRUSTe ultimately determined it could not investigate the complaint since it concerned the collection of personal information from software produced by the company, rather than from the website itself. Critics would argue that this simply reinforces the "hit-or-miss" nature of privacy protection under self-regulation.

Finally, there is the issue of enforcement. If a TRUSTe member fails to comply with the program's requirements, TRUSTe may conduct an audit, revoke the site's license, bring a breach of contract or trademark infringement suit to court, or refer the case to the Federal Trade Commission. None of these penalties provide compensation or redress to the citizen whose privacy has been violated, and it is unlikely that any of these punishments would act as deterrents.

If only a relative handful of sites display the trustmark, revoking a license will have minimal impact on a company. As for pursuing legal remedies:

> *...[I]t costs at least $20,000 [U.S.] to get in the courtroom door. ...The monetary recovery is trivial compared to the cost of litigation [for privacy cases].*"[67]

It should be understood that TRUSTe would not be suing on behalf of an individual for breach of privacy; the organization would sue on its own behalf for trademark infringement. Finally, if TRUSTe intends to refer cases to the FTC for investigation, would it not make sense to grant stronger enforcement powers to that agency? This penalty reinforces the argument for stronger privacy laws, rather than increased industry self-regulation.

The different approaches to privacy protection have resulted in divergent regulatory schemes. It has been suggested that this reflects deeply-rooted cultural differences, with the United States being more concerned with "Big Government" (aka *Big Brother*), while the European Union has been more concerned with "Big Business" (aka *Little Brother*).[68] Since the United States has promoted self-regulation, it has been argued that privacy laws tend to be *ad hoc* or piecemeal responses to specific issues. The result has been a "patchwork" of legislation to cover a few specific types of information, such as financial records, credit reports, video rentals, cable television, educational records, motor vehicle registrations, and telephone records.

Canada, on the other hand, is now apparently following a model of privacy protection that is closer to the European Union. It has formulated legislation based on broad principles of

information privacy, arguably making it more adaptable to social and technological change. Through Bill C-54, Canada is moving toward mandatory privacy protection in the public and private sectors, in compliance with the EU Directive.

Bill C-54 has not been without critics. Some have indicated that it goes too far in promoting privacy at the expense of commerce; others have commented that it does not go far enough in protecting privacy.

From the business perspective, it has been argued that Bill C-54 will impede commercial transactions due to the restrictions on the collection, use and disclosure of information without consent. Since these limitations apply to employee and customer data, the ability of enterprises to sell this information (or even transfer it between related branches) will be detrimentally affected. It has also been pointed out that businesses will face increased administrative challenges, as they attempt to identify all the personal information maintained by the business, the reasons for maintaining the data, and whether the business has consent to use and disclose any or all of the personal information. The main criticism, however, is around the issue of enforcement:

> *Commerce in the borderless world of cyberspace is not a national issue. Enforcement of Canadian privacy regulation will be extremely difficult. If Bill C-54 could somehow be enforced, it could create a competitive disadvantage rather than making Canada an attractive regime for electronic commerce....*[69]

From the privacy perspective, it has been argued that the protection offered through Bill C-54 is too limited, particularly because the legislation is focused on the privacy of data rather than the overall privacy of individuals. Commentators have even suggested that the law itself may violate the spirit of the *Charter of Rights and Freedoms*, since the Privacy Commissioner would be granted broad powers of investigation. These powers include the authority to search for records in places other than a home without a warrant, compel evidence from witnesses, and collect any type of evidence even if it would not be admissible in a court of law. Some critics have concluded:

> *To lobby for it on the grounds that 'some kind of privacy is better than nothing' is shortsighted. While C-54 does have its merits, 'privacy legislation at any cost' is a shameful mantra.*[70]

While Bill C-54 has generated criticism and debate, many privacy advocates and private sector businesses have continued to support the legislation.

Off-Shore Information

While Manitoba has privacy legislation that applies to most public sector organizations and some private sector trustees, the jurisdiction does not extend beyond the provincial border. This has implications for the protection of personal information that is sent "off-shore" to other areas of Canada or the world. Public bodies in Manitoba are signing agreements to send the personal information of Manitobans to other jurisdictions. Once it leaves the province, however, personal information is no longer subject to the oversight of the Ombudsman's Office. For example, if personal information (names, addresses, birth dates, unique identifiers, etc.) provided by a Manitoba public body were lost by a federal agency, our Office would lack the jurisdiction to investigate the actions of the federal body.

This suggests the need for a system of legislative protection and independent oversight that extends beyond provincial and even federal borders. Bill C-54 would extend data protection to areas of the private sector, and to inter-provincial transfers of information. It is likely that the EU Directive will precipitate a new discussion phase on extending protection to Canadian data across provincial and international borders.

ELECTRONIC COMMERCE

The protection of privacy has sometimes been viewed as a barrier to innovation in the public and private sectors. The development of electronic commerce (e-Commerce) via the Internet is a case in point. Statistics indicate that almost 57 per cent of Canadians have a personal computer in their households, and nearly 28 per cent have Internet access.[71] The potential economic activity on the Internet can be estimated by the following figures: in 1998, there were 36,739,000 Internet hosts and 300,000,000 web pages; by March 1999, there were 158,000,000 persons online, with Canadians and Americans totaling 88,000,000 persons online.[72]

Critics of privacy regulation fear that enforcing Fair Information Practices could slow the growth of e-Commerce. It is predicted that regulating the collection, use and disclosure of information would increase costs and damage competitiveness.

There are indications, however, that e-Commerce faces significant hurdles that will only be overcome by *promoting* privacy. A study of Canadian households in 1998, for example, concluded the following:

> *These privacy concerns spill over into the growing field of electronic commerce (e-com). Beyond the technical and marketing challenges inherent in e-com, there is a major stumbling block in terms of Canadians' willingness to share important information electronically. At this stage, Canadians are overwhelmingly reluctant (87 per cent) to provide the basic information (in the form of a credit card number) required to carry out commercial transactions over the Internet.*
>
> *It is not surprising, given these security concerns, that there is agreement with the notion that the government take steps to ensure the security of financial transactions over the Internet. Three in four (74 per cent) Canadians agree with this notion. This sentiment is fairly consistent across all demographic groups.*[73]

It may be that privacy is a necessary component of e-Commerce, rather than a barrier. If so, legislation that promotes privacy could be welcomed by the public and industry.

As custodians of personal information and their information managers adjust to the brave new world of ever-growing computing power and electronic communications without borders, fundamental human values such as privacy are challenging governments and industry leaders to find principled ways and means of conducting business while taking advantage of new technologies. Answers and responses are not clear, and ambivalent attitudes, ambiguous positions, and sometimes contradictory directions often mark their paths. In this context, it is appropriate to return to the survey of 342 Chief Information Officers as reported by a leading information technology company, International Data Group (IDG):

Between a Rock and a Hard Place -- "Competition and Conscience"

CIOs Survey

Tucson, AZ–March 31, 1999–*A new CIO... survey, conducted by IDG's* CIO *magazine, reveals a majority of world's top technology executives are reluctant to provide personal information to Internet vendors, while admitting that it's just this kind of information that is critical to their business success. Sixty percent (60%) of executives assert the ability to track and store information about online consumers outweighs customer privacy concerns; And yet, an equal number (60%) are unwilling to give up privacy in exchange for added customer value or convenience while using the Internet for personal purposes. 'CIOs are between a rock and a hard place with competition and conscience pulling them from both sides,' says Lew McCreary, Director of CIO magazine. 'They want to compete and stay ahead of the curve but are leery of crossing the line between marketing to consumers and encroaching on consumers.'*

The poll of 342 chief information officers (CIOs) and business executives was deployed March 29, 1999, at a CIO Perspectives conference in Phoenix. Poll results also show over two-thirds (73%) of respondents believe the United States should conform to Europe's stricter privacy standards. Established in 1995, the European Union (EU) Privacy Directive prohibits direct marketers from processing sensitive data about consumers without their consent. In spite of the fact that the majority of these execs are in favor of stricter privacy standards, only 9% believe adopting more rigid Internet privacy standards will speed up the development of e-commerce in America. 'These executives are looking for a more principled, not an easier, way to conduct business online,' offers McCreary. 'The strict EU privacy standards would level the e-commerce playing field by dictating where that consumer-privacy line is.' [74]

WRAP-UP

Privacy protection currently depends on piecemeal legislative coverage, voluntary commercial compliance, and public vigilance. Manitoba has taken a significant step toward protecting privacy by enacting legislation that regulates the collection, use, disclosure and security of personal information, and which provides for a substantive oversight mechanism through the Ombudsman's Office. This office also has a duty to inform the public about FIPPA and PHIA. Protection of personal information privacy is a responsibility shared by the custodians of this information *and* the public to whom it belongs individually. Part of this responsibility involves people taking control of their own information, if its privacy is of value to them. We hope that this "Snapshot" will contribute to a general awareness and public discussion of evolving privacy issues.

Endnotes

[1] *The Freedom of Information and Protection of Privacy Act* applies to any "public body". According to s.1, this includes a department, government agency, Executive Council Office, and an office of a minister. It also includes the City of Winnipeg departments. A "public body" will also include a "local public body" (such as school, health care body, and municipality) when the enabling regulation is passed. At the time of writing, the regulation has not yet been proclaimed.

[2] *The Personal Health Information Act* applies to any "trustee". According to s.1, this includes a health professional, health care facility, health services agency and a public body. Therefore, the legislation applies to private sector health professionals who collect or maintain personal health information.

[3] There are three statutes concerning "privacy" in Manitoba. *The Freedom of Information and Protection of Privacy Act* governs the collection, use and disclosure of personal information, while *The Personal Health Information Act* regulates the collection, use and disclosure of personal health information. Under both laws, the Ombudsman is mandated to provide independent oversight of compliance with privacy protection. *The Privacy Act* is limited to providing a legal basis to proceed with a civil action for some breaches of privacy. The Ombudsman's Office is not granted an oversight role for that legislation.

[4] Commentary by Peter Holle, "Hi-tech: Big Benefits or Big Brother?" (*The Winnipeg Sun*, November 30, 1998). Mr. Holle was described as president of the Frontier Centre for Public Policy.

[5] Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms* (October 15, 1998), p.2 at http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

[6] *OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1981, I.L.M. 422, O.E.C.D. Doc. No. C(80)58 final. The document may also be found at http://www.oecd.org/.

[7] Please refer to Appendix A "Fair Information Practices", from Manitoba Culture, Heritage and Citizenship, *Access to Information and Privacy Protection for Manitoba – A Discussion Paper* (May 1996).

[8] For a more complete discussion of *Charter* cases, particularly concerning s.7 and s.8, please refer to Graham Garton, Q.C., *Canadian Charter of Rights Decisions* (July 1998), on the federal Department of Justice website at http://canada.justice.gc.ca/.

[9] Section1 of the *Charter* provides an exception to any right in the document. It states: "The *Canadian Charter of Rights and Freedoms*" 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."

[10] For examples, see *Hunter et al. v. Southam Inc.* [1984] 2 S.C.R. 145 and *R. v. Edwards* [1996] 1 S.C.R. 128. The *Charter*'s impact on privacy is discussed in the *Privacy Commissioner: 1997-98 Annual Report* (Minister of Public Works and Government Services 1998), IP 30-1/1998, pp. 91-97.

[11] Ann Cavoukian and Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* (Toronto: Random House of Canada, 1995), p. 25.

[12] Please see Appendix B for a list of access and privacy statutes across Canada, as well as contact information for the federal and provincial privacy regulatory bodies.

[13] Please refer to Appendix C for a list of web sites for international privacy organizations.

[14] David Banisar and Simon Davies, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice* (1998). To search for this article, please refer to the Global Internet Liberty Campaign (GILC) at http://www.gilc.org/privacy or Privacy International (PI) at http://www.privacyinternational.org/ or Electronic Privacy Information Centre (EPIC) at http://www.epic.org/.

[15] Colin Bennett, Robert Gellman, Nigel Waters and Charles Raab, *Application of a methodology to assess the adequacy of the level of protection of individuals with regard to processing personal data: test of the method of several categories of transfer – final report* (September 1998), pp.96 - 102, at http://www.europa.eu.int/comm/dg15/en/public/index.htm#5. This report was prepared for the European Commission. The legislation in Manitoba was selected as a test case, since it was unique in Canada. The assessment concluded that the law adhered to the major privacy principles under the EU Directive. The main criticism was that PHIA does not provide "seamless protection" for patient records, since some of the heaviest users of patient information (third-party insurers and private employees) are not covered by the legislation.

[16] Ekos Research Associates Inc., *Privacy Revealed* (Ottawa: 1993), p.4.

[17] Louis Harris & Associates, *The Equifax Canada Report on Consumers and Privacy in the Information Age* (Anjou: Equifax Canada Inc., 1995), p.59.

[18] Philippa Lawson and Marie Vallee, "Canadians Take Their Information 'Personal,'" *Privacy Files* I, 1 (October 1995), p. 8.

[19] *Ibid*, p. 7.

[20] Janlori Goldman, "Privacy and Individual Empowerment in the Interactive Age," in Colin J. Bennett and Rebecca Grant (eds.), *Visions of Privacy: Policy choices for the Digital Age* (Toronto: University of Toronto Press, 1999), p.101-102.

[21] Privacy International describes itself as "a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations. PI is based in London, UK, and has an office in Washington, D.C. PI has conducted

campaigns in Europe, Asia and North America to counter abuses of privacy by way of information technology such as telephone taping, ID card systems, video surveillance, data matching, police information systems, and medical records." Its Home Page may be found at: http://www.privacy.org/pi/.

[22] "Privacy and Human Rights: an international survey of privacy laws and practice". This report provides a very useful overview of privacy rights and issues from an international perspective. May be found at http://www.gilc.org/privacy/survey/intro.htm.

[23] Privacy International (PI) states that privacy has many facets and more than one definition, but argues that this should not be taken to imply that the issue lacks importance. According to PI, "privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs. It can be divided into the following facets: • Information Privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records; • Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches; • Privacy of communications, which covers the security and privacy of mail, telephones, email and other forms of communication; and, • Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space." *Ibid.*, p. 4.

[24] Valerie Steeves, "Privacy in Canada: A Public Interest Perspective", *Electronic Commerce and Privacy Legislation: Building Trust and Confidence Conference* (Ottawa, Ontario: February 1999). For more articles on privacy as a human right, please see the Human Rights Research and Education Centre, University of Ottawa, at http://www.uottawa.ca/hrrec/.

[25] Valerie Steeves, "Privacy in Canada: A Public Interest Perspective", *Electronic Commerce and Privacy Legislation: Building Trust and Confidence Conference* (Ottawa, Ontario: February 1999).

[26] Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, *Privacy: Where Do We Draw the Line?* (Ottawa: Public Works and Government Services, April 1997), p.33.

[27] For a more complete discussion of the balance of power in commercial transactions, and the collection of personal information, please see Oscar H. Gandy Jr., "Coming to Terms with the Panoptic Sort" in David Lyon and Elia Zureik (eds), *Computers, Surveillance and Privacy* (Minneapolis: University of Minnesota Press, 1996), p.145.

[28] Tyler Hamilton, "Security breach exposes private Air Miles data", *GLOBEtechnology.com*, January 22, 1999 at http://www.globetechnology.com/.

[29] "Email latest victim of privacy breach," *CNET News.com*, April 16, 1999. Search for this article at http://technews.netscape.com/.

[30] Troy Wolverton, "Another corporate email gaffe", *CNET News.com*, April 21, 1999. Search for this article at http://technews.netscape.com/.

[31] Troy Wolverton, "Privacy at risk in e-commerce rush", *CNET News.com*, April 21, 1999. Search for this article at http://technews.netscape.com/.

[32] Ralph Maddocks, "May this not be an omen," *Le Quebecois Libre*, March 6, 1999, p. 6.

[33] Mike Langberg, "Digital camcorders: The numbers add up", *Seattle Times.com*, April 11, 1999. According to the author, digital camcorders may now be purchased for $800, and will probably continue to fall in price. Search for this article at http://www.seattletimes.com/news/technology/.

[34] Simon Davies, "Europe plans huge spy web", *UK Telegraph Online*, January 7, 1999. Search for this article at http://www.telegraph.co.uk/.

[35] Steve Wright, *An appraisal of technologies for political control*, European Parliament, Directorate General for Research, January 1998. Search for this report at http://www.telepolis.de/

[36] Paul Somerson, "Bombshell", *ZDNet.com*, March 3, 1999. According to the author, individuals can obtain programs to detect working microphones at http://www.pccomputing.com/snoopfix. Search for this article at http://www.zdnet.com/pccomp/.

[37] Roger Clarke, *Information Technology and Dataveillance* (November 1987), p.3. Search for this article at http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

[38] The groups include the American Civil Liberties Union, the National Consumers League, the Consumer Federation of America, Privacy Times, the Centre for Media Education, and the Center for Democracy and Technology. Please see Stephanie Miles, "Movement to halt Pentium III grows", *CNET News.com*, March 5, 1999 and Stephanie Miles, "Groups press agency on Pentium III", *CNET News.com*, March 8, 1999. Search for these articles at http://technews.netscape.com/. Privacy International, the Global Internet Liberty Campaign, the Electronic Privacy Information Centre and Junkbusters supported the boycott as well.

[39] Please refer to Appendix A "Fair Information Practices", from Manitoba Culture, Heritage and Citizenship, *Access to Information and Privacy Protection for Manitoba – A Discussion Paper* (May 1996).

[40] *Privacy Commissioner: Annual Report 1990-1991* (Minister of Supply and Services Canada, 1991), pp.47-51.

[41] Section 46 of *The Freedom of Information and Protection of Privacy Act*.

[42] Roger Clarke, *Dataveillance by Governments: The Technique of Computer Matching* (July 1993), p.5. Search for this article at http://www.anu.edu.au/people/roger.Clarke/DV/MatchIntro.html.

[43] Roger Clarke, *A Normative Regulatory Framework for Computer Matching* (February 1994), p.6. Search for this article at http://www.anu.edu.au/people/roger.Clarke/DV/MatchFrame/html.

[44] Colin J. Bennett, "The Public Surveillance of Personal Data" in David Lyon & Elia Zureik (eds), *Computers, Surveillance and Privacy* (Minneapolis: University of Minnesota Press, 1996), pp. 253-256.
[45] For more information on the concept of the "surveillance society", please see David Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (Chapel Hill: University of North Carolina Press, 1989).
[46] Editorial Staff, "The surveillance society", *Economist*, May 1, 1999. Search for this article at http://www.economist.com/.
[47] John Markoff, "A growing compatibility issue in the digital age: Computers and their users' privacy", *The New York Times*, March 3, 1999. Search for this article at http://www.nytimes.com/.
[48] *Data Mining: staking a claim on your privacy* (Office of the Information Privacy Commissioner of Ontario, 1998), p. 4 and available by searching http://www.ipc.on.ca/.
[49] Sandra Martin, "Oh, pity our ever-shrinking private parts", *The Globe and Mail*, April 10, 1999. This article included a review of *The End of Privacy: How Total Surveillance is Becoming a Reality* (New Press) by Reg Whitaker. Search for this article at http://www.news.globetechnology.com/.
[50] For a discussion of the distribution of bargaining power between corporations and consumers, please see Oscar H. Gandy, "Coming to Terms with the Panoptic Sort" in David Lyon & Elia Zureik (eds), *Computers, Surveillance and Privacy* (Minneapolis: University of Minnesota Press, 1996), pp. 142-146.
[51] Bill 68, the *Act Respecting the Protection of Personal Information in the Private Sector* (1994).
[52] Under *The Personal Health Information Act*, "trustees" include private health care practitioners.
[53] The full title of Bill C-54 is: *An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act*. For a thorough discussion of Bill C-54, please see Murray Long, *Privacy Scan: Analysis and Insight into Bill C-54, Personal Information Protection and Electronic Documents Act* (Murray Long Communications & Policy Consulting, 1999) at http://www.members.home.net/murraylong/.
[54] A committee consisting of business, government, consumer and labour representatives developed the *CSA Model Code for the Protection of Personal Information*. Originally a voluntary code describing the minimum privacy standards for organizations, it has been incorporated as a schedule to Bill C-54. Please search for this document at http://www.csa-international.org/ (As of January 1999, the Canadian Standards Association changed its name to CSA International).
[55] The full title is the *Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of such Data*. It was accepted by the European Parliament on August 20, 1996. Please search for this document at http://www.europa.eu.int/.
[56] Reuters, "EU ministers to rule on e-commerce measures", *CNET News.com*, April 19, 1999. Search for further information at http://technews.netscape.com/.
[57] Please see Colin J. Bennett and Charles D. Raab, "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response", in *The Information Society* (Taylor & Francis, 1997).
[58] Jeremy Quittner, "Would you sell your secrets for free Internet services?", *Businessweek.com*, May 13, 1999. Please search for this article at http://www.businessweek.com/.
[59] Philippa Lawson and Marie Vallee, "Canadians Take Their Information 'Personal,'" *Privacy Files* 1, 1 (October 1995), p. 8.
[60] Courtney Macavinta, "Study: Data privacy policies fall short", *CNET News.com*, May 12, 1999. Search for further information at http://technews.netscape.com/.
[61] Press release, "CIOs grapple with double standard on internet privacy regulation", *CIO Perspectives Conference*, March 31, 1999. The article is available at http://www.cio.com/knowpulse/perspectives99/.
[62] Jason Catlett, "Self-regulation and privacy: Seal programs", *Junkbusters.com*, April 21, 1999. The letter is available on the *Junkbusters* web site at http://www.junkbusters.com/. The letter is cited in a news article by Tim Clark, "BBB Online takes flak for Equifax approval", *CNET News.com*, April 21, 1999. Search for further information at http://technews.netscape.com/.
[63] Richard Raysman and Peter Brown, *Privacy and the Internet* (May 1998) at http://www.ljx.com/securitynet/articles/.
[64] Gerry Miller, Gerri Sinclair, David Sutherland and Julie Zilber, *Regulation of the Internet: A Technological Perspective* (Industry Canada, March 1999), p.16 - 21. Search for it at http://strategis.ic.gc.ca/.
[65] Information provided by the TRUSTe Business Development Manager as of April 15, 1999. For more information about TRUSTe, please see http://www.truste.org/.
[66] Tim Clark, "Truste asked to probe Microsoft", *CNET News.com*, March 16, 1999. Search for this article at http://technews.netscape.com/.
[67] Alan Cohen, *Privacy on the Internet: Concerns Grow, Laws Lag* (March 1998) at http://www.ljx.com/securitynet/articles/.
[68] Colin J. Bennett and Charles D. Raab, "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response", in *The Information Society* (Taylor & Francis, 1997), pp. 258-261.
[69] Richard C. Owens, "Ottawa's privacy protection spells business obstruction", *National Post Online*, April 22, 1999. Search for this article at http://www.nationalpost.com/.

[70] Mark D. Hughes, "Canada's Bill C-54, Civil liberties and Machiavelli", *ISPI Privacy Reporter* 2, 3 (July 1999), p.2.
[71] Ekos Research Associates Inc., *Information Highway and the Canadian Communications Household – Overview of Findings* (February 23, 1998), p.4. See the website at http://www.ekos.com/FEB98.HTML.
[72] Gerry Miller, Gerri Sinclair, David Sutherland and Julie Zilber, *Regulation of the Internet: A Technological Perspective* (Industry Canada, March 1999), p.16 - 21. Search for it at http://strategis.ic.gc.ca/.
[73] Ekos Research Associates Inc., *Information Highway and the Canadian Communications Household – Overview of Findings* (February 23, 1998), p.6 at http://www.ekos.com/FEB98.HTML.
[74] Press release, "CIOs grapple with double standard on Internet privacy regulation", *CIO Perspectives Conference*, March 31, 1999. The article is available at http://www.cio.com/knowpulse/perspectives99/.