

CHAPTER SIX

PRIVACY AS A HUMAN RIGHT: THE WAVE OF THE FUTURE

“The argument that only the guilty “have something to hide” builds on the flawed notion that privacy is about keeping unpalatable secrets. Yet scratch even the most ardent advocate of unfettered technology and you will find a topic that triggers some reserve; personal finances, sexual preferences, medical conditions – we all have “something to hide” and a right to hide it. Truly these matters are no-one else’s (or very few people’s) business. Those who have had the misfortune to live in states that treat the individual’s information as their own understand how this builds social control and weakens the individual.”

Bruce Phillips,
Privacy Commissioner of Canada
Annual Report, June 1999.

Introduction

Privacy is emerging as an important international issue. For those countries implementing new technologies for electronic governance eGovernance in general the electronic delivery of services (eGovernment), having data protection or privacy laws in place is important. It is also clear that the emergence of ever pervasive and intrusive technologies is representing a threat, not only to our privacy, but, our fundamental freedoms as citizens. We are building mechanisms, and accepting them by allowing their implementation and use, in which we are, virtually, potentially building an electronic prison for ourselves. The potential mechanisms for the diminishment of our basic freedoms are now being put in place. These threats make way for the argument that we must enshrine privacy as a basic human right. We need an international convention to achieve this.

Privacy plays an important part in the development of electronic services and the implementation of new technologies. Many countries already have data protection (privacy) laws in place. The European Union has a Directive on the Protection of Personal information that applies to all member states. Other countries, such as Hong Kong for example, have

put in place data protection laws has a law in place which conform with the EU Directive. Malaysia is proposing a law to develop data protection standards. Canada's Parliament has recently passed a Protection of Personal Information and Electronic Documents Act which will come into force in January 2001. Part of Canada's strategy in developing an eCommerce policy is to ensure that laws exist to develop trust and confidence in individuals who come on-line to engage in electronic transactions. *All these laws seek to protect the personal information of the individual from abuse and misuse.* Such protections have become increasingly important with the developments in the on-line world and the massive amounts of personal information being circulated every minute of every day. This chapter looks at the threats posed by these technological advances and why there is a need for some type of individual treaty or convention to protect privacy on the Internet.

In an opening essay to his 1999 Annual Report Canada's Privacy Commissioner, Bruce Phillips eloquently makes the case as to why privacy is not dead, as many have argued. He makes specific references to the Economist's May 1, 1999 article on the *death of privacy* and Professor Reg Whittaker's (York University, Toronto) book 'The End of Privacy: How Total Surveillance is Becoming a Reality'.

The Privacy Commissioner not only makes the case for a robust debate on the need for privacy but also illustrates how acceptances of new technologies are presenting ever-growing threats to our essential freedoms. As he writes, *"the real problem is not the technology, or even some of its seductive promises of convenience, security and efficiency. It is our failure to comprehend the heavy costs that come with the benefits of technology's unchecked insinuation into every facet of modern life. We are effectively building ourselves an electronic Gulag."*

He sees the increased loss of privacy through the intrusiveness of surveillance technologies as concomitant to the threat of the loss of hard won freedoms. He argues that *"perhaps not enough people yet realise that privacy and freedom are inextricably linked; one cannot exist without the other.... But this failure to understand the link is pervasive and leads to many dubious notions taking root."*

Privacy advocates, he contends, use and do enjoy the fruits and benefits of technology but, at the same time, the flaws of technology do not blind the same advocates. They are not Luddites, as many may contend. "Human values," writes the Commissioner, "not technology, must drive the bus. We can build privacy and data security into information tech-

nologies if we are determined to do so.”

He asks, is privacy dead? In answer to the question he poses, he concludes:

“Assuredly it is struggling, but struggle is the eternal and unchanging fate of all freedoms. Freedoms, once lost, can only be regained at the cost of great effort and pain. None can say with certainty that privacy will not be lost here. But if freedom survives at all, so too will privacy, because by definition freedom cannot exist without the right to a life free of surveillance and regimentation.”

Privacy and Human Rights

The message of the Commissioner’s Annual Report is a timely one. It succinctly raises the very real threats that technology poses to both our democratic freedoms and our essential human rights in a free society. The topic of this section is the focus we must begin to put on privacy as a human right as we develop into societies increasingly dependent on the electronic world.

Privacy has now become a major issue internationally. The rise of intrusive technologies and the Internet has resulted in a surge in awareness about the importance of privacy. On the Internet a lot of pressure is being put on companies to develop privacy policies to protect consumers who are liberally sharing their personal information in this new environment. The rush by large corporations to engage in electronic commerce (eCommerce) has meant more personal information is being gathered, shared, sold, and disseminated, than ever before.

What follows is an overview of why citizens appear to be worried about the ways in which their personal selves are being silently abused. Many individuals perceive that their personal information is used in cyberspace in very cavalier ways.

This account reflects only part of the story: how our personal information is bandied around the technological and communication networks of the world. It may seem to some like a fantastic science fiction story rather than a reflection of the reality of the modern world. At any given time, highly computer-literate people, in both government and segments of the private sector, can, within seconds, by using these sophisticated technolo-

gies, know everything about an individual. It is no longer a question that the potential to gather such information is out there but rather how much does it go on?

Yet this capability has been known for sometime. It has been articulated in articles, novels and books. Unfortunately, it has been interpreted to mean that technology is inherently evil and an instrument of control of individuals. In fact, technology is not the problem; it is what people do with the personal information that is at the core of this issue. There is also a paradox built into all this: despite the awareness of the slipshod use of personal information and how much of it is available, people continue not only to use new technologies to give out the most personal details of their lives but seem to enjoy doing it. This does not necessarily hold true with the Internet population where concerns for privacy violations run high. The concerns there are conceivably higher because many people on the Net are, overall, highly literate, earn higher than average incomes, tend to be more highly educated, and are very literate about the technology. They understand what this technology can do and what people can do with it, if protections are not put in place.

In society overall, the perception seems a bit different. The highly driven consumer of the late twentieth century is both the consumer and the consumed of information. On the one hand we seem to want to protect it, on the other we are liberally sharing it. The answer to this is not necessarily stopping the sharing of information but education as to how one's personal information is being used. This has led many technology experts and commentators to conclude that the price of technological convenience is an increasing loss of privacy. Also, others argue that technology is now so pervasive in the industrialized nations of the world that our privacy is now lost forever. Privacy advocates vociferously disagree with this latter view arguing that legislative standards will handle the problem. Many ordinary citizens, not versed in the substantive issues surrounding privacy, know that there is a problem. Surveys indicate that more and more people want to see some mechanisms to protect their privacy in cyberspace.

The transition from the Paper Age to the Digital Age has brought with it new issues for the collection, management and dissemination of information. In the past, especially prior to the rise of the personal computer, seamless international information networks and the Internet, information was often difficult to retrieve.

To get at any kind of information necessitated a laborious process. To

date information from around the globe can be at one's fingertips with the touch of a stroke on a keyboard. Any curious citizen can browse the Internet, use search engines to find out whatever kind of information he/she is seeking from either web sites or a multitude of other Internet related sources.

Searches of databases can allow you to obtain any piece of personal information you want, whether it is on yourself or another. Unless such personal information is specifically protected by statute or government policy, it can be easily obtained. Even those who are technologically literate cannot escape this net. An individual might not go on-line but the information is still ending up in a database somewhere. Personal information is given out almost daily in our personal lives and the collectors of such information, whether a government agency or a private sector organisation, are storing it somewhere in some electronic format.

Thus, all citizens today are intricately intertwined with the global information technology and communication infrastructure even if they do not use or own a computer or ever go on-line.

Whatever transaction we engage in, whether it is using a bank card to withdraw cash or fill out a form (and mail it) to join a book club, the information ends up in a computer. Once entered it can stay in the computer, be shared within a department or organisation or sent anywhere in the world. There are no limitations on the sharing of personal information. Once put into a computer or a network it can be accessed by any number of people. Many countries in the industrialised world have strong public sector privacy laws to protect personal information. Many of the statutes are in need of reform in order to bring them in line with the recent developments in information and communication technologies.

Today we are awash with information. No matter what you want, in all probability you can find it somewhere. Information is ubiquitous; it is in the millions of nooks and crannies on the Internet and on Bulletin Boards and databases around the globe. It can be found in text format on CD-ROM's, as visual data on TV, videos, on-line multi-media images, or in audio. It is as close as the search we want to do. This is the accessible information, that which we do seek out using the multitude of media sources.

In the private sector, this has resulted in a new gold mine for marketers, direct mailing houses, researchers, private investigators and the just plain curious. Data warehouses are now common. It is a practice, called data

mining, engaged in by large and small companies alike around the globe. Any individual with a sophisticated knowledge of the new information technologies, the right equipment and the expertise to use it, can find out everything about you from the day you were born to the present. While few could even be bothered to get such information, there are many companies who want to know many of your personal and spending habits so that specific advertising of products can be marketed directly to you. This occurs every second of every day on a continuing basis around the world. In cyberspace there are no limitations of time or space.

Activity on the Global Information Infrastructure never ceases. For example, an individual can register for a web site in Canada. Another branch of the company might be in Australia. Within seconds that personal information can then be in the data banks of the Australian office. Something in your profile might make you a candidate for a product sold in the company. In turn, the company can then sell your information to any other company in the world because you fit a certain profile. A person interested in skiing could have his/her personal information sold to travel agents, ski manufacturers, airlines, ski resorts or any industry related to skiing. There is no end to the infinite ways in which the information could be used. Personal information is spread out along the corridors of the world's integrated networks. If not protected by a statute barring access or use of it, it is there for the taking.

Another sophisticated method used by many web site owners to gather information about you is through the use of "cookies." Following is a definition and description of "cookies." It is provided by Netscape.

"Cookies are a general mechanism which server side connections can use to both store and retrieve information on the client side of the connection. The addition of a simple, persistent, client-side state significantly extends the capabilities of Web-based client/server applications.

"In human terms this means that Web servers now have (and have had for a long time) the ability to customise a Web site on a person by person basis. Imagine how hard it would be to keep preferences for every browser that has ever visited Yahoo, such a thing couldn't be done if the preferences had to be kept on the Web server it would amount to billions of bytes of data. A much better way to do this is for each browser to keep their own preferences. That's what cookies do.

"Web Browsers set aside a small amount of space on your hard drive to keep these preferences. Then every time you visit a Web site your brows-

er checks to see if you have any pre-defined preferences (cookie) for that server; if you do it sends the cookie to the server along with the request for a web page.

“A browser will not give up its cookie data to any server except the one that set it. If your browser went around spewing all it's cookies to every site you hit this would be a security risk and would make cookies worthless.

Cookies could be used for a lot of things; whether to display a page with frames or text only, shopping cart selections, your name, a username and password, an account number for those sites that charge for viewing. The possibilities are endless, anytime personal data needs to be saved it can be saved as a cookie (if it isn't too long 4000 bytes is the limit).

“Cookies CANNOT be used to get a persons email address. They can save the email address after a browser types it into a form, but they can't GET anything. A cookie is just a holder.”

When you have a cookie in your computer then the next time you go to a web site that put the cookie there it tracks what pages you are looking at. It can then compare this to previous visits. From this it can gather profiles on your interests and this can result in your name ending up on another mailing list. It can get your basic information by asking you to register. It then automatically traps the information on your interests as you peruse the site. This information goes into a database. The information can be made available to other interested marketers. Through computer code other computers can actually talk to each other. In other words, one computer is coded, for example, to respond to anyone interested in skiing. An individual comes in who is a recreational skier and indicates this on a site. That computer can thus be programmed and send this information to another computer in another company or country without a human person being involved. It goes into a database of that company and the process can be continued *ad infinitum*. In this manner all forms of an individual's personal information is snapped up from these databases. This makes the sources of personal information on us in cyberspace almost infinite. It also means our privacy has become almost non-existent. This is why many believe that our privacy is not just vanishing but it has vanished. Privacy legislation, however, effectively applied, can curtail such practices.

The cookie technology in itself can be of use to the Web site owner to determine if the site is offering the right services. If people come in, look

at one page, quickly leave and never come back, this could tell the owner there is something wrong with their design or content on the site. The problem with the cookie technology is when the behaviour of the individual becomes the subject of profiling and the information collected is put up for sale on the Internet. Individuals can erase these cookies from their computers but many are not aware they have the capacity to do this. Erasure of the cookie prevents any future tracking next time you go back to a site. This is one means individuals have to protect their privacy. Erasure of the cookie gives a choice as to whether or not the individual wants to exercise his/her privacy. In Windows 98 cookies can be found by clicking on My Computer. Simply go to the C drive section, click on Windows and in that area you will see the cookie section. Click that on and then delete all the cookies.

It is becoming clear that people are concerned about how their personal information is bandied about and traded like baubles in cyberspace. We are all becoming virtual commodities in an electronic world. People sense that the issue here is greater than privacy. We now are witnessing the development of two separate identities for every individual, our real selves as perceived in the physical world by family, friends, colleagues, etc (to varying degrees), and our virtual selves growing in cyberspace. The latter is based on real data that is, in itself, subjective and not necessarily reflective of our true selves. We have these electronic personalities, or data shadows, which are coming to be interpreted as our real selves.

People are now raising fears and asking questions about the potential for individual harm which new technologies can create for individuals and society at large. Where will these developments take us? We are rapidly becoming technohumans as humanity becomes increasingly integrated with the growing global electronic information technology infrastructure. This makes us subject to decisions being made by invisible controllers of this infrastructure. People are becoming intuitively worried about the forces driving these technological developments. Fears about the loss of our privacy actually reflect a deeper fear of what technology is doing to us as individuals.

There is now abroad in the land the idea that technology is the hope of the future and will lead us to "Elysian Fields" and a better society yet to be dreamed of. Often information issues such as privacy are seen as an impediment to technological development. Many believe individual rights have been parked to the side for these "greater" interests.

Some experts estimate that since 1990 more information has been created

around the world than in all of human history. This growth in our knowledge society is resulting in many benefits for executives, managers, administrators, citizens and societies overall. It is also putting our own personal privacy into a perilous state. The transition from the Paper Age to the Digital Age has brought with it new issues surrounding the usage of personal information. In the past, especially prior to the rise of the personal computer, international information networks, and the Internet, information was often difficult to retrieve, or necessitated a laborious process.

Now information from around the globe can be at one's fingertips with the touch of a stroke on a keyboard. Any curious citizen can browse the Internet, use search engines to find out whatever kind of information he/she is seeking from either web sites or a multitude of other Internet related sources. This creates a whole new dimension to the issue of how personal information is used in today's rapidly changing society. We are in the midst of an information free fall in terms of how our personal information is being used and bandied about.

However, the privacy issue moves far beyond protecting personal information on the Internet. In a larger sense our privacy is being violated daily as new and all encompassing surveillance technologies come on the market.

Surveys show that a large majority of the citizens shopping on-line want to ensure that their personal information is protected, secure and confidential. When surveyed the public asserts strongly of their fear of privacy invasion in our new technological environments. At the same time many of these same people freely use the new technologies that are slowly eroding our freedoms. With each use of these technologies, without debating the long-term deleterious effects on us as a society, we build an ever-tightening electronic noose around society's collective neck. There are many examples of how technology is being used to snoop into our lives from the cameras in the corner shop and in every shopping mall to the ever increasing emergence of personal smart card technologies, being developed by governments, that contain millions of bytes of our personal information.

Technology has meant a wide-scale loss of privacy in comparison to what we enjoyed just twenty years ago. It is not just our personal information that is being abused. We are subject to almost daily scrutiny of our lives. In most countries now video surveillance cameras are accepted as a way of life to combat crime. Computers can now talk to other computers and,

if properly programmed, can exchange information between machines automatically. Computers can monitor every aspect of our on-line activities. In the work place, electronic monitoring of employees is not unusual. In many corporations it is becoming a standard practice in the name of administrative efficiency. In the industrialized countries there are billions of bits of information shared daily. At the same time the prying, ever watchful eye of the camera is increasingly panning more and more of our lives. Web cams can send pictures of an individual in the home or on the street around the world. The problem lies not just with the business world but also with governments who find these technologies more and more persuasive to execute their programs.

Citizens often willingly give up their information so they can receive some benefit that a retailer is offering. Geo positioning satellite (GPS) technology can now send e-mail, faxes and messages to our pagers and, now, even to our cars. But that same technology can also pinpoint exactly where we are at any given time of the day. Whether we are in our car and just a short walk away from where we parked, someone somewhere will be able to know our location. This is just another bit of information that will end up somewhere in a database for possible current or future use by someone.

Employers can monitor every aspect of employees' movements through these technologies. And all of this will be in the name of administrative efficiency, monitoring productivity and being cost effective. In time, governments will find persuasive reasons to also monitor our activities. It appears that society is whistling cheerfully as we descend willingly into the fast approaching dark tunnel of encroaching technological tyranny. The threats to our freedoms are even wider than George Orwell or Aldous Huxley might have ever imagined.

The Ontario Government in Canada has announced plans of the possibility of developing smart cards that will combine a citizen's driver's license, health card, birth certificates and fishing licenses. It will contain a person's personal information on a small chip. The Ontario Government argues that the card will contain the individual's unique fingerprint and thus have the needed privacy and security. But the problem with such technologies is that privacy laws cannot adequately protect the citizen. In time, such unique identifiers can be expanded for usage by more and more government agencies. Soon this could become a card that you must produce on demand. To not do so could tag the citizen "as suspicious" with possibly something to hide because he/she does not want to provide the identity card. The personal information could still be protected by a pri-

vacy act but such protection cannot guard against the human consequences. Such a unique identifier eventually will dehumanise the individual. It has the potential to remove freedom of choice when dealing with a government agency. Cards such as this only serve to diminish the dignity of individuals and rob them of the uniqueness of their individuality.

British Telecom (BT) is developing software, which will allow the computer to determine if you are under stress or upset. The computer can then automatically stop or filter out e-mail or other electronic messages (such as voice mail) coming to the individual. This technology will sound enticing to the worker trying to cope in today's frantic environment. But what could start out as a volunteer application of filtering out messages when upset or under stress could turn into another surreptitious surveillance technology. In the industrialized democracies of the world we are heading towards the total surveillance society as citizens eagerly glom onto the latest technological wizardry.

More importantly, we are growing far too reliant on technology itself and are developing into societies where technology controls daily life as opposed to individuals controlling the technology to better their lives.

In Britain a scientist has developed a chip which he has implanted in himself. The chip is connected to a computer that can monitor his every movement. This same scientist acknowledged there are privacy implications of such a technology. But the frightening aspect of this is that such a technology, once on the market, will end up being used. Only an outcry of public indignation can stop the development and implementation of such technologies.

The irony of all this is that it is occurring in democratic societies where only a few seem to be vigilante enough to speak out and to warn the rest of us of the dangers of where we as societies are taking ourselves. It is important that we continue to debate the issues and educate the citizenry on the dangers posed by the new technologies. This is not an argument to arrest the development of technology but rather to harness its potential harmful results. We need an ongoing debate on these issues. Educating the public is a good start.

Conclusions

Under the current, new privacy law in Canada, the Federal Privacy Commissioner is going to have a mandate to educate Canadians about their new privacy rights. This is perhaps one of the most crucial provisions in the whole legislation. It is through forums, such as in the Annual Report, reports of privacy commissioners around the world and educational programs, that people's awareness will be raised of the need to strike a balance between the development and usage of new technologies and potential threats to our freedoms. Armed with knowledge people can then make their informed decisions. *Current data protection and privacy laws around the world are about the rights of the individual in relation to the protection of their individual privacy.* A right is only as valuable as it is exercised by the citizenry. It is the exercising of our inherent rights that makes our society healthier and democracy stronger. Thus, it will be important to ensure that when electronic services are developed people are informed of their privacy rights either under existing legislation or specific privacy policies if legislation does not exist.

This then leads to the importance of why privacy should be perceived and dealt with as a human right. Canadian Senator Sheila Finestone has drafted a Bill to affirm privacy as a human rights instrument and presented it as a private initiative to the Canadian Senate.

Valerie Steeves, adjunct professor at Carleton University and a well known Canadian human rights and privacy advocate, said that this is a crucial right for all Canadians: *"this Bill is an important step because it provides the umbrella legislation, which places C-6 and the Privacy Act in a human rights context."* It is going to be crucial that privacy is seen and understood in a human rights context if we are going to have a debate about privacy and our fundamental freedoms. Human rights developed within the framework of democratic rights. The two are inextricably linked.

On a wider, international scale it is becoming essential that privacy be enacted as a human right. Current privacy laws are only a finger in the dike trying to hold back the billions of pieces of information now floating around cyberspace. *A broad right is needed that is not only enshrined in law but will create a culture around privacy as a human right.*

The Europeans recognise that privacy, as a human right, is implicit in their laws. Some form of international convention on privacy as a basic human

right is needed.

All these developments suggest a need for an International Privacy and Human Rights Bill. It is essential that such an instrument be agreed upon as a defence against the darker forces of technology that could erode our basic democratic rights. In a civil society it is crucial that we have such instruments that balance our individual rights against the wider forces that drive society. Perhaps the proposed Canadian Bill of Privacy Rights could be the banner to bring this awareness to the wider world beyond those countries that do not have some form of privacy or data protection law. The Canadian proposal could, conceivably, be a model for an International Declaration of the Right to Privacy.