Privacy: The Newest and Oldest Human Right

Bruce Phillips

Seven years ago, a talented academic named David Flaherty, now British Columbia's Information and Privacy Commissioner, wrote a seminal book about protecting privacy in what he called "surveillance societies". Dr. Flaherty argued that individuals in the Western world are increasingly subject to surveillance through the use of private sector and public sector databases. This phenomenon had "negative implications" - a polite understatement to be sure - for the quality of life in our societies and the protection of human rights. In short, life was being transformed by the increasing use of technology for monitoring human activity. As Dr. Flaherty so eloquently summed up the surveillance phenomena, "In the waning years of the twentieth century, our technocratic societies can accomplish what George Orwell could only fantasize about in the aftermath of the Second World War".

Since Dr. Flaherty wrote his book, the movement towards entrenching a surveillance society has continued unabated, aided by society's ever-more-intense search for personal security, efficiency and profit. This, and a host of other factors, have conspired to press privacy's back against the wall.

Tonight I would like to talk to you about this movement, this evolution of society, and its implications for the privacy of all of us. And as I do so, I hope you will reflect on what we stand to lose - as individuals, as a society - if we allow this hard won right to slip form our grasp.

Let me give you just a few examples of how that surveillance society has already become entrenched. On the surface, many of these examples may not seem troubling. They may even seem sensible. But scratch the surface and you may uncover a recipe for the increasing involvement by the state and non-government sectors in your personal life, with little or no offsetting benefit to you or society.

Human Resources Canada announced in October 1996 a plan to match custom forms completed by Canadians returning to Canada to see if they have been cheating on unemployment insurance. Forms from up to three years ago are to be used in this matching process. The original purpose of the customs forms was to identify the value of goods brought back to Canada by returning residents. Until now, travellers have never been told that these forms would be used for the secondary and entirely unrelated purpose of selecting false insurance claims.

- In late September 1996, the federal Justice Minister, the Honourable Allan Rock, introduced amendments to the Criminal Code to allow the government to ask a

judge for authority to place an electronic device on an individual to monitor his or her movements. The device can be used if there are reasonable grounds to fear that the individual will commit a serious personal injury offence against someone else, even if the purported victim is not named. The individual being monitored need not have been charged with or convicted of any offence.

- An American direct marketing company sells a list with the addresses of some 80 million U.S. households by ethnic group. Among the 35 groups that can be singled out with this list are Armenians and Jews. The information that can be purchased includes the number of children and their age range. Wouldn't a terrorist love to get a hold of that list!
- Another service, available for a fee through the Internet, offers to help track down any of 160 million individuals living in the United States. Among the information the service will provide is the address, telephone number, names of household members and dates of birth, and the listing of up to 10 neighbours.
- Under a program called Pharmanet, records of all prescriptions issued to residents of British Columbia are stored in a provincial database, linked by name to the individual receiving the prescription. B.C. residents have no right to opt out of the database. The collection by government of what could be highly sensitive medical information about them is compulsory. The Pharmanet program seeks, among other things, to protect individuals from obtaining conflicting prescriptions, since the use of conflicting prescriptions is a major cause of hospital admissions in that province. In addition, the information from this mandatory collection can be shared with others, such as the police, for purposes completely unrelated to the health care of the individual.
- In one high school in Indiana, school policy requires random drug testing of students who participate in various activities, including parking on school property, taking part in open lunch and cheerleading. President Clinton announced before the November election that his administration officials are to develop a plan that would involve drug testing all those who apply for a driver's licence.
- The United States military has begun a program to take DNA samples from two million American servicemen, to enable the military to identify the remains of battle casualties. The military will also make DNA available to the police for criminal investigations, thus providing in one instant what the police could never otherwise hope to obtain - a DNA database of about two million individuals who are not even remotely suspected of having committed a crime.
- In the United Kingdom, some 200,000 surveillance cameras are in use; in at least one city, they have also been installed in residential neighbourhoods and have

the ability to look into residences; many of these cameras have powerful zoom lenses and the ability to see at night; in Toronto, on October 25, 1996 some striking workers conducting their "Day of Protest", largely a peaceful, lawful activity in that city, were at some locations being monitored by camera from a central office in downtown Toronto.

- At least one Canadian pharmacy chain has developed a database containing information about prescriptions issued to its customers; we do not know for what purposes that information is being used or if it is being shared with or sold to other companies or the police.
- Technology can now make a digital image of your face, store the image, then link up with a camera to scan a crowd - for example, a political demonstration - for your presence. The manufacturers of one such imaging system claim that by 1997 their product will be able to scan a database of 50 million faces in less than a minute.
- A device known as an ion scanner can - without your knowledge - electronically sniff your luggage for contraband when you enter the country.
- A device known as a passive millimetre wave detector uses a form of radar to scan beneath clothing. The system can detect items such as guns and drugs from a range of 12 feet or more. It can also look through building walls and detect activity. Of course, the subject of the search need never know that he or she is being searched.
- Voice recognition technologies can pluck your telephone conversations from the sky, then transcribe those conversations, all with very little need for labour intensive human involvement.

Some of the measures I have described have chilling overtones. Some may seem a little absurd. Others may not seem too troubling at first glance. Some will clearly appear to be beneficial. But let's take a closer look at some of these ostensibly beneficial forms of surveillance.

Take surveillance cameras for example. It is difficult to argue that a single surveillance camera in an underground parking garage constitutes a grave threat to privacy. It may even prevent some criminal activity, make people feel safer when they enter such garages, and help catch those who commit crimes in such places.

However, when the number of cameras increases to the point that the ordinary citizen cannot go about their lawful daily business without being captured on camera somewhere, this form of surveillance begins to inhibit the normal activities of those citizens. Simon Davies, one of today's most outspoken critics of intrusive technologies, describes the use of technologies of surveillance, particularly the widespread use of

cameras, as a kin to the issuance of a general search warrant on the entire population. In a society such as ours that prides itself on limiting the powers of the state to intrude into our lives, the growth of this type of largely unregulated surveillance is alarming, to say the least. And the question remains: Do surveillance cameras reduce crime, or do they simply displace it to areas not already under surveillance?

What about such devices such as the ion scanner and the passive millimetre wave detector devices that can conduct searches of people completely without their knowledge? That may be fine if a person is a terrorist, but is it fine for the vast number of us - the large majority - who are not terrorists? There is no requirement for a warrant to undertake such a search with these devices. Yet, if this technology did not exist, a police officer would almost certainly need a warrant to conduct a similar search of your body.

Mr. Justice La Forest, in his dissent in the Supreme Court of Canada decision R. v. Silveira (1995), noted the degree of protection from arbitrary searches afforded the home: "It is surprising that nearly four hundred years after the Semayne's case (1604), 5 Co. Rep. 91, 77 E.R. 194, there should be any debate about the matter. That case firmly enunciated the principle that 'a man's home is his castle', and that even the King himself had no right to invade the sanctity of the home without the authority of a judicially issued warrant. That principle has remained ever since as a bulwark for the protection of the individual against the state. It affords the individual a measure of privacy and tranquility against the overwhelming power of the state..."

How will our Supreme Court react to technologies such as the passive millimetre wave detector, which allows agents of the state to see through the walls of the very home that has long been protected from arbitrary intrusions by the state?

And what about drug testing? Mandatory drug testing has been lauded as the quick fix to drug abuse in the workplace and everywhere. Yet sound evidence to show that drug testing solves anything is absent.

At the same time, drug testing involves a serious privacy intrusion - the surrender of a bodily substance to allow a government or employer to ascertain one's past conduct with whatever substances are deemed a social evil. Dealing effectively with drug abuse requires education, support, treatment and, in some cases removing the conditions that may well cause or exacerbate problems that lead to harmful levels of drug use. Massive mistrust and surveillance through drug testing are not the answer. Unfortunately, however, drug testing is made out to be the neatest "solution" to what is a complex issue - the use of drugs in ways that can harm others.

The technology leading to today's surveillance society is changing the nature of human relationships. It is threatening the very existence of a hard won and fundamental human

right - the right to privacy. We may have come a long way, but unfortunately in the wrong direction, since the days when one's home was one's castle and when one had control over one's own body.

What is Privacy?

Privacy has been part of the vocabulary of human rights advocates for almost a century. Privacy is not simply an abstract notion that intrigues academics, confounds their students, but matters to no one else. Intrusions into our personal lives have concrete, real-world consequences. They shape how we lead our lives. The limits of our personal privacy define in part the limits of our freedom. As Mr. Justice La Forest stated in the Supreme Court of Canada's 1990 Duarte decision, "it has long been recognized that this freedom not be compelled to share our confidences with others is the very hallmark of a free society". Columbia University Professor Alan Westin is equally forceful, describing privacy as being at the heart of liberty in a modern state.

What is privacy? In one sense, it means protection against physical intrusions against the person, such as assaults or physical searches by police. It can be the protection from intrusion against one's personal property, such as one's home. It may mean the right to protection from surveillance by cameras or eaves dropping devices or, perhaps, researchers. It may mean the right not to have your personality appropriated.

Privacy is also about information. In the 1988 Supreme Court of Canada Dyment decision, Mr. Justice Lamer cited a government task force report about the importance of privacy of information: "This notion of privacy (of information) derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain as he see fit".

In modern society especially, Mr. Justice Lamer continued, retention of information about oneself is extremely important. If the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated.

And privacy is a non-renewable resource. Once you lose it, it cannot be regained or regenerated. Just look at Prince Charles and Lady Diana, the players in one of the world's favourite soap operas. Can either of them ever hope to regain the privacy that they have lost through the interception of their telephone calls? On a more plebian level, can someone who tests positive for HIV regain control of this sensitive personal information once it has been released into the community? A loss of control over this information can have devastating consequences for a person already facing an overwhelming crisis. Can someone whose personal information is intercepted on the information highway ever hope to re-establish control over that information?

What is Protecting Our Privacy?

In the past 50 years, privacy has taken its place alongside other human rights in international conventions, constitutional law, federal and provincial legislation and professional codes of conduct. Our courts too have increasingly come to speak of the privacy rights of Canadians.

Article 3 of the Universal Declaration of Human Rights states that everyone has the right to life, liberty and security of the person. Article 12 states that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks upon his honour and reputation. The International Covenant on Civil and Political Rights contains almost identical language.

Canada has also sought to enhance privacy protection through vehicles other than international law. In 1984, Canada joined 22 other industrialized nations by adhering to the OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data. The guidelines are intended to harmonize data protection laws and practices among OECD member countries by establishing minimum standards for handling personal information. Unlike the other international instruments mentioned above, which protect privacy rights in general, the Guidelines protect only one aspect of privacy - the privacy of personal data.

The OECD Guidelines apply both to the public and private sectors. However they constitute a voluntary code of conduct. They are not legally binding on governments or the private sector of OECD member countries.

Canada also has constitutional privacy protections, perhaps not through explicit language in the Canadian Charter of Human Rights and Freedoms, but through thoughtful interpretations of its provisions by our courts, including the Supreme Court of Canada. Two sections of the Charter are most relevant - section 7, the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice, and section 8, the right to be secure against unseasonable search and seizure.

Court decisions interpreting the Charter as offering privacy protection have most often arisen in the context of the criminal law. However, the Supreme Court of Canada has also made it clear that the Charter is relevant to privacy concerns outside of the criminal context.

In a recent Supreme Court of Canada criminal appeal, R. v. Edwards, Mr. Justice La Forest reinforced the notion that the Charter protects a broad range of privacy interests:

> As I see it, the protection accorded by s.8 (the right to be secure against unreasonable search or seizure) is not in its terms limited to searches of premises over which an accused has a personal right to privacy in the sense of some direct control or property. Rather, the provision is intended to afford protection to all of us to be secure against intrusion by the state or its agents by unreasonable searches or seizures, and is not solely for the protection of criminals through the most effective remedy will inevitably protect the criminal as the price of liberty... (The section 8 right) is a right ensuring to all the public... Moreover, s.8 does not merely prohibit unreasonable searches or seizures, but also guarantees to everyone the right to be secure against such unjustified state action. It draws a line between the rights of the state and the rights of the citizen, and not just those of an accused. It is a public right, enjoyed by all of us. It is important that everyone, not only an accused, that police (or what is even more dangerous for the public, other agents of the state) do not break into private premises without warrant.

Canadians also benefit from federal data protection legislation, the Privacy Act. As Privacy Commissioner of Canada, I have the responsibility of overseeing the application of the Act. The Act regulates the federal government's collection, use and disclosure of personal information about Canadians. It also gives individuals the right to see the personal information about them held by government, and to request that the information be corrected if it is wrong.

In a nutshell, the Act seeks to ensure that the federal government complies with internationally accepted practices regarding the handling of personal information. The Act has provincial counterparts in most provinces - New Brunswick is still a notable exception - and foreign counterparts in most Western countries. Ontario's privacy legislation, for example, regulates the collection, use and disclosure of personal information by the provincial and municipal governments.

Canada also has a host of other laws protecting privacy, ranging from privacy torts in four provinces to credit reporting laws and laws governing medical confidentiality. But faced with modern threats to privacy, our laws remain dangerously porous. Outside Quebec, there exists no general private sector data protection legislation. True, an industry group operating under the umbrella of the Canadian Standards Association has produced an excellent voluntary code regulating the handling of personal information by the private sector. However, the code remains voluntary.

As well, our laws have not kept up with advances in technology. We now face the slightly absurd situation where it is a criminal offence in Canada to eaves drop without the consent of one person being listened to. Yet it is not a criminal offence to conduct highly intrusive video surveillance of those same persons as long as you don't listen to

what they say. Many other intrusive applications of technology similarly have not yet been addressed by the legal system.

The Complicating Factor

Protection of privacy is thus hindered by incomplete and ineffective privacy laws. That alone is not an insurmountable problem. Legislators do react to privacy concerns, albeit slowly. However, a host of other factors have conspired to impede effective privacy protection in Canada.

The first such factor is the public mood - or rather, the apparent shift in the public mood towards what a cynic might call "personal security at all costs, security at any cost". One need only listen to the tirades in Parliament about the need to get tough on the perceived increases in crime. Privacy is being converted into the poor cousin in debates about public security. Privacy interests that are seen as hindering effective law enforcement or endangering public security, whether they are in truth a hindrance or not, are too often swept aside. Examples include the publicizing of ID of sex offenders, drug testing or prisoners, electronic bracelets for those who have not been charged with or convicted of any offence.

The second factor is the call for efficiency, the sirens of our times. Governments are looking to increase the efficiency and reduce the cost of their operations. These are noble goals, but in too many cases privacy becomes an afterthought, at best, and a victim at worst.

For example, government databases hold a wealth of information about individuals. That information can be sold to private sector interests, offsetting the cost of government operations. As well, to enhance the efficiency of their operations, governments are looking for new ways to mix and match data. Take data about those who travel abroad and compare it with a database of individuals who claimed unemployment insurance to see if they were really available for work as they stated. Compare unemployment insurance files with income tax returns to detect fraud. Ensure that people are not abusing their welfare privileges.

The third factor militating against rational protection of privacy is the marketing power of the high technology industry. Surveillance technology industries stand to gain hundreds of millions of dollars by marketing their products as vehicles for enhancing security or productivity or some other social good. These industries stand to gain millions by persuading the public that surveillance cameras are an indispensable tool for ensuring security and protecting property. The biotechnological testing industry stands to make enormous sums of money by persuading governments and companies alike - despite evidence to the contrary - that drug use is out of control and that their drug protection services will keep the barbarians at bay.

Nowhere in the marketing pitch for these technologies is one likely to hear an acknowledgement that they carry a large, hidden, price - your privacy. And the marketing power of these industries, their drive for profits, overwhelms the less well financed (to make an understatement) voices of individuals and organizations concerned about protecting privacy. The Davids standing up to these corporate and governmental Goliaths are privacy commissioners, human rights organizations and individual citizens. None of these has the financial clout to counter sophisticated marketing campaigns aimed at extolling the virtues of surveillance, while ignoring the profound damage that surveillance does to our privacy.

Privacy is also increasingly being cast as the villain, as the impediment to protecting society. Too often I have heard government officials say they cannot release information because of the Privacy Act, even if that release would serve the public interest. Nor do the privacy laws of most provinces. In fact, the federal Act provides a procedure by which the head of a government institution can release information, whether the Privacy Commissioner would think the release was wise or not. Our society is also mesmerized by technology. This "gee-whiz" attitude about technology makes it more like a mere toy, and less like what it can become in the wrong hands - an intrusive weapon.

Another in this long list of factors preventing a rational approach to protecting privacy is our unwillingness to reconsider laws and policies that can operate only if supported by massive privacy intrusions. One controversial area, to be sure, is our laws on illegal drugs. Few areas of law enforcement generate such massive levels of surveillance and intrusion as our drug laws. Yet, how often do we stop to consider the privacy consequences of these laws? How often do we look for means of dealing with drugs in our society that might prove equally effective, but that would not necessitate some of the most egregious privacy intrusions imposed by Western governments on their citizens?

Defeatism is also impediment to protecting privacy. "The technology is here. We can't stop it . Why bother trying?" In addition, there is a disturbing new element in the current debate over privacy and technology. It is the line of argument that we have to re-think privacy, we have to accommodate our expectations of what can remain private in the wake of advancing technology. But no one ever said that it was going to be easy to protect your rights. Losing rights is simple. Protecting them requires elbow grease. This lesson we too often forget - until it is too late.

Privacy advocates have also learned that mere existence of an intrusive technology or a collection of personal information will invite its further use. Just as gas expands to fit its container, potentially intrusive technologies will expand to meet their technological boundaries.

Among the greatest challenge that we face in trying to secure privacy results from the diffuse nature of privacy threats. rarely can we identify a single incident, a single technology, a single government policy that constitutes such a threat to privacy in our society that the public springs to its feet in protest. Instead, intrusions insinuate themselves into our daily lives, one by one, bit by bit. Yet the end result is equally dramatic - a profound loss of privacy.

In this sense, responding to privacy concerns is much like protecting the environment. It would be extreme, and inaccurate, to argue that someone who dumps a few litres of toxic effluent into the Saint John River is causing an environmental catastrophe. However, as more and more individuals dump effluent into the River, their actions do become catastrophic.

Protecting privacy requires a similar type of discourse. It is difficult to argue that a particular use of your personal information by the federal government - comparing, or "matching" information about you held by two separate government departments, for example - constitutes a grave threat to your privacy in and of itself. However, as more and more departments engage in this process, we move from isolated incidents of "data matching" to wholesale "data mining", where all information held by your government can be drawn together for a particular government purpose. You find yourself under comprehensive surveillance.

And of course you have nothing to hide. But that is not the point. Even if you have nothing to hide, you have a great deal to lose. You have your autonomy, your sense of anonymity, your right to go about your business unmolested. And even if you have nothing to hide, surveillance will subtly alter your behaviour. Take away your privacy and you take away your dignity, your control over your life.

Avoiding the Death of Privacy

I have tried to identify just some of the sobering challenges, the impediments to protecting privacy as we head into the third millennium. But how about a few solutions?

Filing the gaps left by our patch work of privacy laws is an obvious priority. In particular, Canada needs an extension of data protection laws to cover the information handling practices of the private sector. Except for Quebec, no Canadian province has had broad data protection legislation governing the private sector. I am greatly encouraged that the federal Minister of Justice is committed to introducing private sector data protection legislation for industries subject to federal regulation. But filing the gaps through legislation alone is not enough.

Human rights advocates - the Davids facing the Goliaths - must accept a central role in pushing privacy to the fore in the human rights and political discourse of our country.

We need to remind Canadians that privacy is not a peripheral matter. It is a core value from which so many other democratic rights flow.

Perhaps most important, we need to shape an ethical framework for society, infused with respect for privacy. Like it or not, technology has changed our relationships as human beings. What ethical principles must we instill in our society to adapt to this change, yet protect this right?

A central principle must be the rights of citizens to use privacy enhancing technologies. Just as technology can intrude, technology can protect against intrusion. Access to cryptography in personal communications, access to anonymous digital cash in financial transactions, for example, should be the norm. Where possible, features to enhance privacy should be built into the technology. And access to such privacy features should be free. Individuals should not have to justify their desire ti use these technologies to protect their privacy. Instead, those who wish to limit the use of these privacy enhancing technologies should bear the burden of proving the need to do so.

All citizens should have the right to demand that any potentially intrusive technology be subject to an assessment of its privacy implications - sort of privacy audit - before it is introduced to run amok in society.

Above all, we must not allow ourselves to be seduced by the flawed logic that more surveillance means a better, more secure, society. One can only hope that the memory of the authoritarian regimes that scarred the planet for much of this century, and the awareness of those that continue to do so today, will help us retain a distaste for surveillance societies. In the end, as we prepare to enter the next millennium, I hope that we be able to look upon the remaining years of the millennium as the years that gave birth to a new appreciation of privacy, not the era that presided over the dying gasps of a fundamental human right.

References

Banisar, David. "Big Brother Goes High-tech", in Covert Action Quarterly. 56, 1996.

Flaherty, David. 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.

Catalyst Direct Marketing. October 28, 1996. http://www.catalyst.com/ ethnic.htm

Montreal Gazette, Sunday, October 20, 1996, p. 1.

MacDonald, S. "The Role of Drugs in Workplace Injuries", in Journal of Drug Issues. 25 (1995): 703-22.

National Drug Strategy Network, "Newsbriefs", April 1996, p. 21.

People Finder. October 28, 1996. http://www.infoam.com/lpf.htm

Simon, Davies. Monitor: Extinguishing Privacy on the Information Superhighway. Sydney: Pan Macmillan Australia Pty Limited, 1996.

Westin, Alan F. Privacy and Freedom, 1970.