PRIVACY IN A "SURVEILLANCE SOCIETY"

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".[1] 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 in monitoring human activity. Dr. Flaherty eloquently summed up the surveillance phenomenon saying, "[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."[2]

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 movement and a host of other factors have transformed the right to privacy. Society stands to lose this very right if it remains inattentive to these changes.

A few examples of how a surveillance society has already become entrenched can be seen in many sectors of one's personal life. On the surface, many of these examples may not seem troubling; they may even seem sensible — but scratch the surface and you may uncover increasing involvement by the state and non-government sectors in your personal life, with little or no offsetting benefit to you or to society.

- In October 1996, a newspaper story revealed that Human Resources Development Canada was matching names of unemployment insurance claimants with customs forms completed by Canadians returning to Canada to see if they have been cheating on unemployment insurance. Forms dating back three years will 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 detecting false unemployment insurance claims.

---

*Privacy Commissioner of Canada. This paper is based upon the text of the Seventh Dr. Bernie Vigod Memorial Lecture, delivered at St. Thomas University, Fredericton, New Brunswick on 7 November 1996.

[1]D. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (Chapel Hill & London: University of North Carolina Press, 1989).

[2]*Ibid.* at 6.

• An American direct marketing company sells a list of the addresses of some 80 million U.S. households, sorted by ethnic group.[3] Among the 35 groups which may be singled out using this list are Armenians and Jews. The information that can be purchased includes the number of children and their age range. A concern which immediately comes to mind is the list's accessibility to terrorists.

• Another service, available for a fee through the Internet, offers to help track down any of 160 million individuals living in the United States.[4] Among the information the service will provide is the address, telephone number, names of household members, dates of birth and a list 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 and linked by name to the individual receiving the prescription.[5] B.C. residents have no right to opt out of the database. This collection by the government of what could be highly sensitive medical information is compulsory. The Pharmanet program seeks, among other goals, to protect individuals from obtaining conflicting prescriptions, since the use of conflicting medications is a major cause of hospital admissions. In addition, this information 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.[6] President Clinton announced before the November election that his administration officials are to develop a plan that would involve drug testing for individuals who apply for a driver's license.[7]

• The United States military has begun a program to take DNA samples from two million American service people to enable it to identify the remains of battle casualties. The military will also make this record available to the police for criminal investigations, providing in one instant what the police could never

---

[3]"Catalyst Direct Marketing: the future difference" (February 1997), http://www.catalystdm.com/ethnic.htm (accessed 28 October 1996).

[4]The service is called "People Finder". "Information America" (1997), http://www.infoam.com (accessed 28 October 1996).

[5]See the discussion of Pharmanet in British Columbia, Office of the Information & Privacy Commissioner, *Annual Report 1994-95* (Victoria: Queen's Printer, 1995) at 57 where the Information and Privacy Commissioner of B.C. criticizes the compulsory nature of the scheme.

[6]National Drug Strategy Network, (April 1996) Newsbriefs at 21.

[7]A. Mitchell, "Clinton Links Driver's license to drug test" *The [Montreal] Gazette* (20 October 1996) A1.

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.[8] At least one city has installed them in residential neighbourhoods, where they 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 25 October 1996, some striking workers conducting their "Day of Protest" were being monitored by camera from a central office in downtown Toronto, even though it was largely a peaceful and lawful activity.

• At least one Canadian pharmacy chain has developed a database containing information about prescriptions issued to its customers. The purposes for which the information is being used, or if it is being shared with or sold to other companies or the police, is yet to be determined.

• Technology can now make a digital image of your face, store the image, then link up with a camera to scan a crowd for a match. Such a device could easily be used to scan a crowd at a political demonstration to determine whether a particular individual is present. The manufacturers of one such imaging system claim that by the end of this year, 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 secretly detect contraband in luggage when a person enters the country.

• A device known as a passive millimeter wave detector uses a form of radar to scan underneath clothing. Such a 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.[9] The subject of the search may never know that he or she is being searched.

• Voice recognition technologies can pluck your telephone conversations from the air waves then transcribe those conversations, without the need for human involvement.

Some of these measures have chilling overtones, some may seem a little absurd, or others may not seem too troubling at first glance. Some will clearly appear to be beneficial. A closer look, however, at some of these ostensibly beneficial forms of

---

[8]S. Davies, *Monitor: Extinguishing Privacy on the Information Superhighway* (Sydney: Pan Macmillan, 1996) at 207.

[9]D. Banisar, "Big Brother Goes High-tech" (1996) 56 Covert Action Quarterly 10.

surveillance will give one a different understanding of the impact that technology has on privacy.

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 and help catch those who commit crimes. However, this form of surveillance begins to inhibit the normal activities of ordinary citizens when the number of cameras increases to the point that ordinary citizens cannot go about their lawful daily business without being captured on camera somewhere. Simon Davies, one of today's most outspoken critics of intrusive technologies, describes the use of technologies of surveillance, like cameras, as akin to the issuance of a general search warrant on the entire population. In a society such as ours which prides itself on limiting the powers of the state, the growth of this type of largely unregulated surveillance is alarming. A question remains: do surveillance cameras reduce crime or do they simply displace it to areas not already under surveillance?

Other noteworthy devices are the ion scanner and the passive millimeter wave detector. These devices can conduct searches of people without their knowledge. They may be useful to identify terrorists, but are these measures necessary for the rest of the population? No warrant is required to search with these devices, something a police officer almost always requires to conduct a search of a person's body.

Justice La Forest, in his dissent in the Supreme Court of Canada decision, *R.* v. *Silveira*, noted the degree of protection from arbitrary searches afforded to homeowners:

> It is surprising that nearly four hundred years after *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 principles 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 tranquillity against the overwhelming power of the state; see also *Entick v. Carrington* (1765), 19 St. Tr. 1029. *It is a fundamental precept of a free society.*[10]

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

Another concern related to the protection of privacy is drug testing. Mandatory drug testing has been lauded as the quick fix to drug abuse in the workplace and

[10][1995] 2 S.C.R. 297 at 319 [emphasis added].

elsewhere. Yet sound evidence to show that drug testing solves these types of problems is conspicuously absent.[11]

At the same time, drug testing involves a serious intrusion on privacy. The surrendering of a bodily substance to allow a government or employer to ascertain one's past contact with illegal substances infringes this right. Dealing effectively with drug abuse requires education, support, treatment and, in some cases, removing the conditions that cause harmful levels of drug use. Widespread mistrust and surveillance through drug testing is not the answer to drug abuse. Unfortunately, drug testing is posited as the best "solution" to what is a complex issue — the abuse of drugs.

The technology leading to a surveillance society is changing the nature of human relationships. It is threatening the very existence of a hard-won and fundamental human right to privacy. Society has come a long way, but 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 and confounds their students. 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 large part the limits of our freedom. As Justice La Forest stated in the Supreme Court of Canada's 1990 decision, *R.* v. *Duarte*, "it has long been recognized that this freedom not to be compelled to share our confidences with others is the very hallmark of a free society."[12] Columbia University professor Alan Westin is equally forceful, describing privacy as being at the heart of liberty in a modern state.[13]

Privacy, in one sense, means protection against physical intrusions against the person, such as assaults and physical searches by police. It can be the right to protection from intrusions on one's property, such as one's home. It may mean the right to protection from surveillance by cameras, eavesdropping devices or even researchers. It may mean the right not to have your personality appropriated.

---

[11]See *e.g.* the criticism of the methodology used to evaluate the effectiveness of many drug testing programs, in S. Macdonald, "The Role of Drugs in Workplace Injuries: Is Drug Testing Appropriate?" (1995) 25 Journal of Drug Issues 703.

[12][1990] 1 S.C.R. 30 at 53.

[13]F. Westin, *Privacy and Freedom* (New York: Atheneum, 1970) at 349-50

This right is also about information. In the 1988 Supreme Court of Canada decision of *R.* v. *Dyment*, Justice La Forest cited a government task force report about the importance of privacy of information: "'This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit.' In modern society especially," Justice La Forest continued, "retention of information about oneself is extremely important."[14] If the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated.

Privacy is a non-renewable resource. Once you lose it, it cannot be regained or regenerated. For instance, Prince Charles and Princess Diana became 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 plebeian level, can someone who tests HIV-positive regain control of this sensitive personal information once it has been released into the community? Losing control over this information can have devastating consequences for a person already facing an overwhelming crisis. Also, those who have personal information intercepted on the information highway may never be able to re-establish control over that information.

What is Protecting our Privacy?

In the past fifty 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 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.[15] Article 12 states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."[16] The *International Covenant on Civil and Political Rights* contains almost identical language.[17]

---

[14][1988] 2 S.C.R. 417 at 429.

[15]United Nations, *Human Rights: A Compilation of International Instruments* (New York: United Nations, 1978) at 1 (UN Doc. ST/HR/1/Rev.1, Sales No. E.78.xlv.2)

[16]*Ibid.* at 2

[17]*Report of The Canadian Delegation Review of Canada's Second and Third Reports on The International Covenants on Civil Political Rights* (Ottawa: Multiculturalism and Citizenship Canada, 1990) (United Nations Human Rights Committee, Geneva 23-24 Oct. 1990)

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.*[18] 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. The *Guidelines* are not legally binding on governments or the private sector of OECD member countries.

Canada also has constitutional privacy protections. The Supreme Court has interpreted certain sections of the *Canadian Charter of Rights and Freedoms* to include these protections.[19] There are two sections of the *Charter* that are most relevant: section 7 expresses 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 protects the right to be secure against unreasonable search or seizure.

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

In a recent criminal appeal, *R.* v. *Edwards*, 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 even though the most effective remedy will inevitably protect the criminal as the price of liberty for all. ... [The section 8 right] is a right enuring 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; see *R. v. Dyment*, [1988] 2 S.C.R. 417, at p. 427. 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

---

[18]Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: Organisation for Economic Co-operation and Development, 1981).

[19]Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11.

> us. It is important for 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.[20]

In addition, Canadians benefit from federal data protection legislation, the *Privacy Act*.[21] The Privacy Commissioner of Canada has the responsibility of overseeing the application of this Act. The Act regulates the federal government's collection, use and disclosure of personal information about Canadians. It also gives individuals the right to examine the personal information about them held by the 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 still being 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 the privacy torts in four provinces, to credit-reporting laws and laws governing medical confidentiality. However, faced with modern threats to privacy, our laws remain dangerously porous. Outside Québec, 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, that code remains voluntary.

As well, our laws have not kept up with advances in technology. We now face the slightly absurd situation in that it is a criminal offence in Canada to eavesdrop without the consent of one of the persons being listened to, yet it is not a criminal offence to conduct highly intrusive video surveillance of those same persons as long as one doesn't listen to what they say. Many other intrusive applications of technology have not yet been addressed by the legal system.

The Complicating Factors

The protection of privacy is hindered by incomplete and ineffective privacy laws. That fact 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.

---

[20][1996] 1 S.C.R. 128 at 149-150.

[21]R.S.C. 1985, c. P-21.

The first such factor is the public mood. There is an 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 increase in crime. Privacy is being converted into the poor cousin in debates about public security. Privacy interests that are perceived 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 publicizing the identity of sex offenders, the drug testing of prisoners and the placing of electronic bracelets on those who have not been charged with or convicted of any offence.

The second factor is the call for efficiency, the siren song of our times. Governments are looking to increase the efficiency and reduce the cost of their operations. These are worthy 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 own operations, governments are looking for new ways to mix and match data. For instance, governments will gather 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 to work as they stated. Also, they compare unemployment insurance files with income tax returns to detect fraud and 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, 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 testing services will solve this problem.

Nowhere in the marketing pitch for these technologies is one likely to hear an acknowledgement that they exact a large, hidden price known as our privacy. The marketing power of these industries, and their drive for profits, overwhelms the less well-financed 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 such surveillance does to our privacy.

Privacy is also being cast increasingly as the villain, as an 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. The Act does not prevent such a release of information in 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 wise or not.

Our society is also mesmerized by technology. This gee-whiz attitude about technology makes it seem more like a toy and less like an intrusive weapon when the technology is in the wrong hands.

Another in this long list of factors preventing a rational approach to protecting privacy is society's unwillingness to reconsider laws and policies that can operate only if supported by massive privacy intrusions. One controversial area is the law on illegal drugs. Few other areas of law enforcement generate such massive levels of surveillance and intrusion. Often people do not stop to consider the consequences of these laws for privacy. Society fails to look for means of dealing with drugs 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 an 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 and that we have to accommodate our expectations of what can remain private in the wake of advancing technology. No one ever said that protecting your rights was easy. Losing rights is simple. Protecting rights requires elbow grease. This lesson is too often forgotten until it is too late.

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

Among the greatest challenges that we face in trying to secure privacy is 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 that it pushes the public to its feet in protest. Instead, intrusions insinuate themselves into our daily lives, one by one, bit by bit. Yet, the end result is still 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 St. John River is causing an environmental catastrophe. However, as more and more individuals dump effluent into the river, their actions do become catastrophic. Similarly, it is difficult to argue that a

particular use of one's personal information by the federal government, such as comparing or "matching" information about an individual held by two separate government departments, constitutes a grave threat to privacy in and of itself. However, as more and more departments engage in this process, governments move from isolated incidents of "data matching" to wholesale "data mining", where all information held about someone can be drawn together for any purpose. The result is a comprehensive surveillance scheme.

Of course we have nothing to hide, but that is not the point. Even if someone has nothing to hide, she has a great deal to lose. One's autonomy, sense of anonymity and the right to go about her business unmolested are severely challenged. Even if one has nothing to hide, surveillance will subtly alter a person's behaviour. Take away someone's privacy and you take away their dignity and their control over their life.

Avoiding the Death of Privacy

This paper has identified just some of the sobering challenges and impediments to protecting privacy in the third millennium. Are there any solutions?

Filling the gaps left by the patchwork of present 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 Québec, no Canadian province has 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. However filling 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. They need to remind Canadians that privacy is not a peripheral matter. It is a core value from which many other democratic rights flow. Perhaps most importantly, there is a need to shape a new ethical framework for society, infused with respect for privacy. Like it or not, technology has changed our human relationships. What ethical principles must be instilled to adapt to this change, yet protect this right?

A central principle must be the right of citizens to use privacy enhancing technologies. Just as technology can intrude, technology can protect against intrusion. Access to cryptography in personal communications and 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. Access to such privacy-enhancing features should be free. Individuals should not have to justify their desire to 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 — a 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 these remaining years will be looked upon 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.