# Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance

*Arthur J. Cockfield**

*The author raises questions about potential threats to our democratic order that may arise from advancements in surveillance technology. Among the developments that concern him are the increasing power of investigators to conduct surveillance, the enhanced ability of the public and private sectors to share information and the steady growth in the sophistication of surveillance technology. At the same time, there is less scrutiny of surveillance practices by independent bodies. The author argues that these factors are combining to make surveillance of individuals dangerously easy. He warns that this may erode key democratic values, particularly freedom of expression and the right to privacy.*

*The author reviews the* Personal Information Protection and Electronic Documents Act (PIPEDA), *and concludes that while it is a good first step, it falls short by not adopting the European Union's strict approach to consent. As a result, further measures are needed to ensure that democratic values are adequately preserved, such as stronger laws dictating how government and private agencies collect and store information as well as greater accountability of government to its citizens. In addition, to help ensure such accountability, the author argues that there should be a method of tracking government searches for information. Finally, the author suggests an alternative system under which the personally identifying elements of collected information are removed and stored separately, accessible only upon independently verified grounds.*

Introduction

I. Laws That Governed the Watchers Before September 11th

A. *Government: Reasonable Expectations and Private Spaces*

B. *Commerce: Ubiquitous Information Collection Practices*

---

* Assistant Professor, Queen's University Law School. On October 4, 2001, an earlier draft of this paper was presented at a Queen's University Surveillance Project seminar and the author would like to thank the seminar participants for the many helpful comments that he received. In addition, the author wishes to thank David Lyon, Don Stuart, Bernie Adell and David Freedman for comments on an earlier draft. This article was also discussed during a Joint Program of Sections on Civil Rights, Intellectual Property and Law and the Social Sciences, at the American Association of Law Teachers Annual Meeting in New Orleans on January 6, 2002. Jason Young provided extremely helpful research assistance for this work.

(i) Laws That Govern Private Sector Watchers
(ii) Private Sector Reaction to Privacy Concerns
(iii) The *Personal Information Protection and Electronic Documents Act*
C. *Governing the Watchers in an Era of Technology Change*
II. **The New World: Weakened Legal Control Over Government Watchers**
A. *Reduced Expectations of Privacy*
B. *Reduced Judicial Scrutiny*
C. *No Government Oversight*
D. *The Promotion of New Surveillance Technologies*
E. *Government Watchers and the Growing Surveillance Network*
III. **The Road Ahead: Watching the Watchers**
A. *The Watchers and the Erosion of Privacy*
(i) The Repression of Expression
(ii) Stifling Political Dissent
B. *Policy Response: Watching the Watchers*
(i) Strengthening Private Sector Surveillance Laws
(ii) Using a "Code is Law" Approach to Watch the Watchers
(iii) Watching the Watchers Through Enhanced Reporting
Conclusion

# Introduction

As a result of the terrorist attacks of September 11th 2001, Canada and other nations have expanded surveillance measures in order to address perceived security concerns.[1] In many circumstances, governments have increased or propose to increase the use of technology to gather detailed information about the personal identity of suspected terrorists and criminals. Examples include increased surveillance of Internet activity, increased surveillance of public spaces by digital video cameras and the adoption of national identification cards embedded with biometric information. At the same time, governments have weakened traditional

1. Governments are responding to a post-9/11 reaction that embraces enhanced surveillance as a requirement for better public protection. This view was supported by a number of polls suggesting that a majority of citizens want government(s) to take pro-active security measures. See *e.g.*, Ingrid Peritz "The War On Terror: Ipsos-Reid/The Globe and Mail/CTV Poll" *The Globe & Mail* (29 December 2001) A10; Shawn McCarthy "N. American War on Terror Seen As Threat To Privacy" *The Globe & Mail* (13 December 2001) A12; John Ibbitson "Why Racial Profiling is a Good Idea" *The Globe & Mail* (3 June 2002) A15.

legal protections against unauthorized police searches and are increasingly turning to private sector databases to access previously collected personal information.

In this article I argue that this combination of legal change and technological development could seriously impede privacy rights and lead to an erosion of democratic values.[2] Specifically, there is a risk that fear of increased government scrutiny of public and private spaces will inhibit certain forms of speech, including political dissent. Furthermore, an environment of intrusive technological surveillance may lead to a less democratic government as citizens find it difficult to hold lawmakers and enforcers accountable for surveillance practices that are not reviewed by independent actors, such as judges. Individual liberty is weakened to the extent that the emerging surveillance network encourages a lack of public accountability and makes individuals less trusting of their governments and more fearful of expressing political dissent. Together, these concerns highlight a fundamental question for any political system: "Who watches the watchers?"[3]

This article is organized as follows. Part I briefly reviews the right to privacy in the context of public and private sector surveillance under Canadian law and discusses uses of surveillance technologies. The analysis reveals that government searches have traditionally been subject to strict legal protections, while in the private sector there are far fewer restraints on the collection of personal information. However, recent Canadian federal legislation strives to comprehensively regulate business information collection practices.

Part II discusses how legal controls over public sector surveillance in Canada have been weakened after the events of September 11th. In some circumstances there is no longer a need to obtain authorization from an

---

2. Concern about the erosion of privacy rights due to increased government surveillance and/or technological developments preceded September 11th, 2001. See *e.g.*, Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) [*Privacy and Freedom*]. For a discussion of the rise of surveillance in America, primarily by government, see Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Random House, 2000).

3. The question is derived from ancient Latin saying: *Sed quis custodiet ipsos custodes?* See Decimus Junius Juvenal, *Satires* (Paris: Collection des universités de France, 1964) at Book VI, Line 347.

independent judge prior to the conduct of surveillance. Further, governments are using or proposing to use emerging information technologies to track vast amounts of personal information. Implementation of a surveillance network may continue to create problems even if the traditional legal protections are put back in place.

Part III discusses how a well-meaning public/private surveillance regime could lead to undesired and anti-democratic results such as inhibiting speech and creating a lack of accountability for potentially abusive state actions. In order to manage the growing tension between security and privacy, I will recommend several measures to encourage mechanisms to watch the watchers. These measures could include (i) enhanced legal protections against private sector surveillance to give consumers more control over the disclosure of personal information that could end up in government hands; (ii) increased oversight and reporting mechanisms for government surveillance; and (iii) laws to mandate technological steps to protect personal data within large databases from unauthorized access.

# I. Laws That Governed the Watchers Before September 11th

In examining the pre-September 11th legal regime that protected privacy, I will focus on the legal constraints on efforts by government and commercial actors to scrutinize personal behaviour under Canadian law.[4] It is useful to touch on American legal and technological

4. Federal and provincial laws that affect privacy interests are extensive and complex. This review touches only upon some of the main laws in this area. Throughout this article, the term "privacy" means the ability of an individual to control what personal information others may know. However, the definition of privacy is somewhat contentious and other commentators have come up with more expansive and more narrow definitions. For discussion, see Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (Ithaca: Cornell University Press, 1997) at 46-61. In order to focus the discussion on the different legal regimes surrounding government and private sector surveillance, the analysis in this section of the paper ignores the increased blurring of public and private roles as governments, for example, subcontract traditional state activities to the private sector. For discussion, see *e.g.*, Dan Schiller, *Digital Capitalism:*

developments for two main reasons. First, Canadian regulators may emulate American laws, policies and technologies, or American and Canadian regulators may agree to harmonize them in order to ensure that cross-border economic flows are not disrupted.[5] For example, after September 11th, 2001, Canada and the United States agreed on a border security plan that involves collecting and sharing information and intelligence on border crossers and other individuals.[6] Second, American surveillance technologies might be used to gather information on Canadian citizens and residents. A Canadian civil liberties group has warned: "We could soon find ourselves in a situation where all personal information on Canadians will be in the hands of, and managed centrally by American security agencies unaccountable to Canadian Parliament and the Canadian public."[7]

Part I also pays particular attention to the new Canadian legislation, the *Personal Information Protection and Electronic Documents Act*,[8] which governs the information collection practices of private industry and which takes full effect on January 1, 2004.[9] Finally, Part I concludes by

---

*Networking the Global Market System* (Cambridge: MIT Press, 2000) at 37-88 (discussing global efforts to privatize traditional government services).

5. The policy of regulatory emulation results from the fact that Canada and the United States have developed closely integrated economies and Canadian economic success is perceived to depend in large part on ties to the U.S. market. For discussion, see Arthur J. Cockfield, "Tax Integration under NAFTA: Resolving the Conflict between Economic and Sovereignty Interests" (1998) 34 Stan. J. Int'l L. 39.

6. See Department of Foreign Affairs and International Trade, News Release, "Canada-U.S. Smart Border Declaration" (12 December 2001) online: DFAIT <http://www.dfait-maeci.gc.ca/anti-terrorism/declaration-en.asp> [DFAIT].

7. See the International Civil Liberties Monitoring Group, Report, "In the Shadow of the Law: A Report by the International Civil Liberties Monitoring Group in Response to Justice Canada's 1st Annual Report on the Application of the Anti-terrorism Act (C-36)" (14 May 2003) [In the Shadow of the Law]. The ICLMG is a broad coalition of Canadian groups (civil rights advocates, NGOs, churches, unions and environmental advocates) that monitors the application of Canada's anti-terrorism legislation.

8. *Personal Information Protection and Electronic Documents Act*, R.S.C. 2000, c. 5 [*PIPEDA*].

9. Under the new law, the consent of Canadian consumers is required before the collection of personal information by industry. See *PIPEDA*, *ibid.* which was effective January 1, 2001 for certain federally regulated industries and covering all businesses

discussing the relationship between the law and surveillance technologies.

### *A. Government: Reasonable Expectations and Private Spaces*

Under early English common law, an individual's home was protected from unwarranted scrutiny by the sovereign, hence the saying "a man's home is his castle."[10] Even if one was not fortunate enough to live in a castle, the law restricted the King from barging through the front gates for anything but criminal matters.[11] Over time, the view developed that the home was the centre of an appropriately private sphere and that what went on within its walls was generally not the state's concern.[12]

---

operating in Canada as of January 1, 2004 unless "substantially similar" provincial legislation already applies, as in Quebec.

10. "The house of every one is his castle, and if thieves come to a man's house to rob or murder, and the owner or his servants kill any of the thieves in defence of himself and his house, it is no felony and he shall lose nothing." *Semayne v. Gresham* (1604) 5 Co. Rep. 91a at 93a, 77 E.R. 194 at 198 (K.B.).

11. William Pitt, Earl of Chatham, in a speech on the *Excise Bill* in the English Parliament said, "[t]he poorest man may in his cottage bid defiance to the Crown. It may be frail; its roof may shake; the wind may enter; the rain may enter—but the King of England cannot enter—all his forces dare not cross the threshold of the ruined tenement!" John Bartlett, *Familiar Quotations: A Collection of Passages, Phrases & proverbs Traced to their Sources in Ancient and Modern Literature*, 10th ed. (Boston: Little, Brown & Co., 1919) at 365. See also *Entick v. Carrington and Three Other King's Messengers* (1765), 19 How. St. Tr. 1029: "By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing."

12. Richard Turkington & Anita Allen, *Privacy: Cases and Materials*, 2d ed. (Houston: John Marshall Law, 1998) at 5. See also *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 [*Hunter*] (broadly construing the protection against reasonable searches in part to protect privacy against unjustified state intrusion). In Canada, the protection against unreasonable searches extends to the person and not the place: "This is inherent in the idea that privacy is not a right tied to property, but rather a crucial element of individual freedom which requires the state to respect the dignity, autonomy and integrity of the individual." The degree of privacy which the law protects is closely linked to the effect that a breach of that privacy would have on the freedom and dignity of the individual. Hence, a person is entitled to an extremely high expectation of privacy in relation to his or her bodily integrity (as in *R. v. Stillman*, [1997] 1 S.C.R. 607) or residence (as in *R. v. Feeney*, [1997] 2 S.C.R. 117). Individuals have been held to have a much lesser expectation

While there is no explicit constitutional right to privacy in Canada, the Supreme Court of Canada has noted the critical role of privacy in democracies:

> [S]ociety has come to realize that privacy is at the heart of liberty in a modern state . . . Grounded in a man's physical and moral autonomy, privacy is essential for the well-being of the individual . . . The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.[13]

The Court has also recognized that:

> [P]rivacy concerns are at their strongest where aspects of one's individual identity are at stake, such as in the context of information "about one's lifestyle, intimate relations or political or religious opinions."[14]

---

in relation to a vehicle in which they were merely passengers (as in *R. v. Belnavis*, [1997] 3 S.C.R. 341) or to apartments which they were a visitor (as in *R. v. Edwards*, [1996] 1 S.C.R. 128). See also *Schreiber v. Canada (Attorney General)*, [1998] 1 S.C.R. 841 at para. 19.

13. *R. v. Dyment*, [1988] 2 S.C.R. 417 at 427. For discussion of the Canadian approach, see Don Stuart, *Charter Justice in Canadian Criminal Law*, 3d ed. (Scarborough: Carswell, 2001) at 218. In the United States, the *Bill of Rights*, U.S. Const. amend. I-X, has been interpreted by the U.S. Supreme Court to grant a limited right to privacy that prevents a government from interfering with personal decisions such as abortion and contraception. However, as in Canada, there is no general right to privacy. See *e.g.*, *Bowers v. Hardwick*, 478 U.S. 186 (1986). In *Olmstead v. United States*, 277 U.S. 438 (1928) [*Olmstead*], U.S. Supreme Court Justice Brandeis wrote in his dissent:

> The makers of our Constitution . . . conferred, as against the Government, the right to be let alone—the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

Brandeis' dissent became the majority view in *Katz v. United States*, 389 U.S. 347 (1967) at 361 [*Katz*]. In the landmark case of *Griswold v. Connecticut*, 381 U.S. 479 (1965) at 483, the court declared that an individual has a constitutional right to privacy in certain circumstances. The Court located this right within the "penumbras" or "zones" of freedom created by an expansive interpretation of the *Bill of Rights*. Douglas J. first expressed the "penumbra metaphor" in his dissent in *Poe v. Ullman*, 367 U.S. 497 (1961) at 517. The right to an abortion is grounded in part in privacy rights: *Roe v. Wade*, 410 U.S. 113 (1973).

14. *R. v. Mills*, [1999] 3 S.C.R. 668 at 722.

The Supreme Court has articulated its views on privacy in the context of constitutional protection offered against government searches.[15] For instance, section 8 of the Canadian *Charter of Rights and Freedoms* reads: "Everyone has the right to be secure against unreasonable search or seizure."[16] The Fourth Amendment to the American *Constitution* contains a similar prohibition against unreasonable searches.[17] These constitutional protections generally prohibit government agents from using technologies to scrutinize private activities unless the police secure a search warrant issued based on the probability of criminal activity.

Courts have interpreted these constitutional protections to take technological developments into account. For example, the Ontario Court of Appeal has ruled that the police use of airplanes equipped with Forward Looking Infra-Red (FLIR) to detect heat emanations indicative of marijuana growing operations constituted a search that required prior judicial authorization under section 8 of the *Charter*.[18] The search warrant obtained as a result of the FLIR search was therefore not lawfully granted, and the conviction of the accused was quashed.

---

15. In addition to prohibitions against illegal police searches, privacy interests are related to a number of other important constitutional rights in Canada. For example, privacy plays an important role in the promotion of other *Charter* rights such as section 2 (freedom of conscience, religion, thought, opinion and freedom of peaceful assembly and association), section 7 (the right to life, liberty and security of person), section 9 (the right not to be arbitrarily detained or imprisoned), section 11 (the right against self-incrimination), and section 15 (the right to equal treatment and benefit of the law without discrimination).

16. *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11., s. 8 [*Charter*].

17. U.S. Const. amend. IV reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

18. *R. v. Tessling*, (2002) 63 O.R. (3d) 1 (C.A.), leave to appeal to S.C.C. granted, (2003) S.C.C.A. No. 116. In *Kyllo v. United States*, 533 U.S. 27 (2001) [*Kyllo*], the U.S. Supreme Court held that police use of thermal imaging to scan for high intensity grow lamps inside private residences constitute an impermissible search.

The general thrust of decisions by Canadian courts is to protect "reasonable expectations" of privacy.[19] A person may, for example, expect to be left alone in her home or when she conducts a transaction at her bank, but arguably has reduced expectations of privacy when she posts opinions in a newsgroup from her home or when she is jogging in the park.[20] Accordingly, a court might not have any concerns about government-initiated video surveillance in a downtown urban center.[21]

Beyond these constitutional protections, Canada has federal laws that prevent public agencies from collecting, using or disclosing personal information in many circumstances. The federal *Privacy Act*[22] often prevents the federal government from accessing or sharing personal information. This legislation also permits individuals to access, request or annotate personal information about them that is held by federal public organizations.

In addition, Canada has a federal Privacy Commissioner whose mandate includes monitoring violations of privacy laws and ensuring that information gatherers are held accountable for their actions. There is no equivalent overseer in the United States, although several federal agencies perform some of the same functions. Among them are the Office of Management and Budget, which participates in setting privacy policies for federal agencies, and the Federal Trade Commission, which provides guidance and oversight for private sector privacy practices. Both countries also have provincial or state legislation that restricts the

---

19. See *e.g.*, *Hunter*, *supra* note 12. See also David E. Steinberg, "The Drive Toward Warrantless Auto Searches: Suggestions from a Back Seat Driver" (2000) 80 B.U.L. Rev. 545.

20. Section 8 of the *Charter* and the Fourth Amendment of the U.S. *Constitution* have been interpreted to protect "people not places or things" such that what a person knowingly exposes to the public, even in her own home or office, is not is not protected, but what she seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. See *e.g. Hunter, supra* note 12; and *Katz*, *supra* note 13.

21. But see Privacy Commissioner, News Release, "Privacy Commissioner Launches Charter Challenge" (21 June 2002), online: Privacy Commissioner of Canada <http://www.privcom.gc.ca/media/nr-c/02_05_b_020621_e.asp>; Privacy Commissioner, Opinion 02/04, "Opinion by Justice Gérard La Forest" (5 April 2002), online: Privacy Commissioner of Canada <http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp>.

22. R.S.C. 1985, c. P-21.

collection and distribution of information including the sale of personal information collected for the purpose of driver licensing.[23]

### *B. Commerce: Ubiquitous Information Collection Practices*

#### (i) Laws that Govern Private Sector Watchers

Information technology developments have enhanced the ability of the private sector to collect detailed information about customers and employees. Businesses have historically tracked their customers' behaviour (*e.g.*, through credit card purchases) and have often sold this information to third parties. Information technology developments now permit the collection and storage of an enormous quantity of detailed transactional information, and also allow for relationships to be drawn between formerly discrete identities.[24] Through information technologies, companies can cheaply and easily collect information about consumer transactions and connect it to provide a detailed picture of a person's identity.

Consider the impact of the Internet. Industry currently collects information on website visits through various data mining techniques (*e.g.*, "cookies"),[25] and posts tens of billions of banner ads each month targeted at customers.[26] Over 90% of commercial websites gather some form of data on website visitors.[27] By June 2000, the largest online

---

23. See *e.g.*, *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31.

24. See *Privacy and Freedom*, *supra* note 2; Simon Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (Cambridge: O'Reilly, 2000) at 70, for a historical discussion of the emergence of detailed digital dossiers or "data shadows".

25. The use of "cookies" has been debated since 1996. Cookies are small data files placed on the computers of visitors to a website. The remote computer hosting a website can update them—effectively having limited privileges to write data to the user's computer. Cookies can collect information for marketing, such as the which pages are visited and how often. Cookies also remember passwords and permit users to personalize a site. Consumers can set web browsers to reject all cookies (or to control cookies through more advanced settings). However, this can be difficult for new users to figure out.

26. Federal Trade Commission, "Online Profiling: A Report to Congress" (June 2000), online: Federal Trade Commission <http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf>.

27. *Ibid.*

marketing company, Doubleclick Inc., had compiled databases on roughly 88 million American households to assist in these direct marketing campaigns.[28] A U.S. court has ruled that Doubleclick.com can legally place "cookies" on the hard drives of consumers for data mining purposes, although this type of monitoring would likely be considered an illegal search if conducted by government.[29]

In contrast to laws that apply to government, there have historically been far fewer common law or legislative restraints on industry information gathering practices. Canadian common law protections against invasion of privacy are similarly limited such that "it would appear that invasion of privacy in Canadian common law continues to be an inceptive, if not ephemeral, legal concept, primarily operating to extend the margins of existing tort law."[30]

Common law doctrine and statutory regimes have historically offered fewer protections against private sector data collection in part because non-governmental surveillance, at least on the surface, does not appear to erode democratic values; businesses are simply trying to do a better job of selling their products to consumers who can always refuse to buy them.[31] As a result, commentators often assert that the real threat to

---

28. Tom McNichol, "Double Agents" *Wired* 8:6 (June 2000) 124, online: Wired <http://www.wired.com/wired/archive/8.06/mustread.html?pg=6>.

29. See *In re DoubleClick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001). The case involved a class action lawsuit against a company that provides Internet advertising products and services. The plaintiffs claimed that DoubleClick violated federal laws and state laws, including common law invasion of privacy, unjust enrichment, and trespass to property. The court dismissed the federal claims and declined jurisdiction over the state law claims. See also *Dwyer v. American Express Co.*, 273 Ill. App. 3d 742 (1995), holding that the practice of selling customer information does not constitute an unreasonable intrusion into the seclusion of an individual under the privacy invasion tort.

30. *Ontario (Attorney-General) v. Dieleman* (1994), 117 D.L.R. (4th) 449 at 688 (Ont. Ct. Gen. Div.). For a discussion of the common law and provincial statutory protections for privacy rights in Canada, see William Charnetski, Patrick Flaherty & Jeremy Robinson, *The Personal Information Protection and Electronic Documents Act: A Comprehensive Guide* (Aurora: Canada Law Book, 2001) at 16-21.

31. But see David Lyon, "The World Wide Web of Surveillance: The Internet and Off-World Power-Flows" (1998) 1 *Information, Communication & Society* 91 at 105 (arguing that private sector surveillance leads to social sorting and reinforces existing inequalities of power and access).

privacy and democratic rights is an increase in government surveillance.[32] As discussed throughout this article, new surveillance technologies increase the risk of abusive state surveillance that erodes democratic values.

(ii) Private Sector Reaction to Privacy Concerns

The private sector has responded to these consumer privacy concerns through a number of different avenues. For example, Internet users can use browsers such as Microsoft's Internet Explorer and Netscape's Navigator to set privacy preferences to reject cookies. In addition, a number of trusted third party intermediaries issue seals of approval for websites that follow self-defined privacy guidelines.[33] Other programs, such as the Platform for Privacy Preferences Project (P3P), offer the potential for greater privacy protection by permitting consumers to have more control over the information they divulge to the private sector.[34] Further, a number of companies provide "identity management" technologies to Internet users to mask or anonymize their identities. In many circumstances, these anonymizing technologies permit the company to reveal the identity of its customers upon being presented with a search warrant or subpoena. In contrast, some technologies do not permit even the privacy company holding the data

32. See *e.g.*, David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (Chapel Hill: University of North Carolina Press, 1989) at 375, concluding that government surveillance is the primary threat to privacy rights.

33. See *e.g.*, online: TRUSTe <http://www.truste.org>; online: Better Business Bureau <http://www.bbbonline.com>; online: CPA Web Trust <http://www.cpawebtrust.org>.

34. Developed by the World Wide Web Consortium, P3P is emerging as an industry standard providing a simple, automated way for users to gain more control over the use of personal information on websites they visit. At its most basic level, P3P is a standardized set of multiple-choice questions, covering all the major aspects of a website's privacy policies. Taken together, they present a clear snapshot of how a site handles personal information about its users. See Platform for Privacy Preferences (P3P) Project, online: W3.org <http://www.w3.org/P3P/>.

to access it, hence frustrating any potential police investigation.[35] In the current environment, political pressure may reduce the use of such technologies because they could permit terrorists or other criminals to communicate without fear of detection. Any potential restrictions on anonymizing technologies may, however, be counter to principles of freedom of expression that are given broad constitutional protection.[36] For example, people who want to criticize government practices can use anonymizing technologies to mask their identities if they fear state reprisal.[37]

(iii) The *Personal Information Protection and Electronic Documents Act*

With the exception of Québec, Canada generally pursued a self-regulatory approach to private sector privacy protection until the passage of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*).[38] As of January 1, 2004, all companies doing business in Canada will have to obtain explicit or implicit consent prior to collecting or distributing personal information.[39]

---

35. For example, Montreal-based Zero-Knowledge Systems once used a "pseudonymous IP network" in which no one party had access to all the necessary bits needed to reconstruct a user's identity or transactions, except the user herself. The company discontinued the sale of this product after September 2001. See Ian Avrum Goldberg, *A Pseudonymous Communications Infrastructure for the Internet* (Ph.D. in Comp. Sci. Thesis, University of California at Berkeley, 2000) [unpublished], online: U.C. Berkeley <http://www.isaac.cs.berkeley.edu/~iang/thesis-final.pdf>.

36. See *e.g.*, *R. v. Sharpe*, [2001] 1 S.C.R. 45; *Canada (Human Rights Commission) v. Taylor*, [1990] 3 S.C.R. 892; *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995); *Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton*, 536 U.S. 150 (2002).

37. See generally A. Micheal Froomkin, "Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases" (1996) 15 U. Pitt. J of Law & Comm. 395.

38. *Supra* note 8.

39. On that date, *PIPEDA* applies to federal works, undertakings or businesses and, otherwise, every organization in respect of personal information that collects, uses or discloses such information in the course of commercial activities. On January 1, 2002, *PIPEDA* applied to all organizations that collect, use or disclose health information. *PIPEDA* applies to all businesses operating in Canada beginning January 1, 2004 unless those organizations are already covered by "substantially similar" provincial legislation.

A brief examination of some of the main provisions of *PIPEDA* is necessary to understand the recent changes to the legal regime surrounding Canadian private sector information-gathering practices.[40] *PIPEDA*'s stated purpose is, in part, to protect privacy interests in "an era in which technology increasingly facilitates the circulation and exchange of information."[41] It only applies to private sector actors that collect "personal information" in the course of "commercial activity."[42]

---

But see Stephanie Perrin *et al.*, *Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law, 2001) at 22 (indicating that "legal, medical, or security reasons may make it impossible or impractical to seek consent").

40. The United States and Canada have taken different paths with respect to information collection practices used by commercial actors. The U.S. generally follows the industry self-regulation model, under which companies are expected to regulate their own information gathering techniques. Self-regulation has been promoted as efficient and equitable. In theory, a company will align its information gathering techniques with the privacy expectations of its customers: it is just good business to do so. In reality, there may be a number of market failures—information asymmetry, imperfect competition, lack of transparency and so on—that may prevent industry from getting it right. For discussion of self-regulation versus formal regulation in the context of online privacy, see Arthur J. Cockfield, "Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation" 85 Minn. L. Rev. 1171 (2001) at 1200-1221. Despite the emphasis on self-regulation in the United States, there is a trend toward greater administrative oversight by the Federal Trade Commission. Prior to the terrorist attacks, legislation envisioning enhanced privacy protection was winding its way through federal and state governments. The Federal Trade Commission also encourages fair data collection practices under the governance of four guiding principles: notice, choice, access and security. In addition, federal U.S. legislation uses a sectoral approach to protect certain forms of personal information such as financial records, medical records, and information concerning children. See *No Child Left Behind Act of 2001*, Pub. L. No. 107-110, 115 Stat. 1425 (2002) (protections against the commercial profiling of schoolchildren); *Treasury and General Government Appropriations Act*, Pub. L. No. 107-67, 115 Stat. 554 (2002) (prohibits federal government agencies from snooping into individuals' web browsing habits); *21st Century Department of Justice Appropriations Authorization Act*, Pub. L. No. 107-273, 116 Stat. 1758 (2002) (requiring the Department of Justice to release detailed reports on the use of the Carnivore Internet surveillance program); *Health Insurance Portability and Accountability Act (HIPAA) of 1996*, Pub. L. No. 104-191, 110 Stat. 1936 (1996); and *Gramm-Leach-Bliley Act of 1999*, Pub. L. No. 106-102, 113 Stat. 1338 (1999). For discussion, see Peter P. Swire, "The Surprising Virtue of the New Financial Privacy Law" 86 Minn. L. Rev. 1263 (2002).

41. *Supra* note 8 at s. 3.

42. *Ibid.* at s. 2(1).

Personal information is defined as "information about an identifiable individual," not including the "name, title or business address or telephone number of an employee of an organization."[43] "Commercial activity" is defined as "any particular transaction, act or conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."[44] *PIPEDA* does not apply to any organization that uses personal information solely for journalistic, artistic, or literary purposes.[45]

*PIPEDA* strives to encourage fair information management practices. It encourages accountability by mandating data collector responsibility for the personal information of a data subject, including information that has been transferred to an unrelated third party. Further, the collecting organization must designate an individual to be accountable for the collection practices. It must also ensure that the personal information is as accurate, complete and up-to-date as is necessary for the purposes for which it will be used. The information must also be stored in a secure fashion by, for example, protecting electronic records with encryption and audit trails.[46] In addition, upon written request, companies must provide consumers with access to personal information stored by the organization, for the purpose of correcting any errors.

The general approach of *PIPEDA* is that consent must be obtained before certain personal information can be collected, used, or disclosed. The expectations of a "reasonable person" determine whether consent must be explicit or if it may be implied based on the circumstances.[47] A subscriber might reasonably expect that a magazine would have implied consent to solicit subscription renewal, but if the magazine wished to sell a list of its subscribers to a third party, it would be necessary to seek additional, explicit consent because that purpose would be inconsistent with the original consent.[48]

---

43. *Ibid.*

44. *Ibid. PIPEDA* also applies to the collection of personal information about employees of any "federal work, undertaking or business."

45. *Ibid.* at s. 4(2)(c) and s. 7(1)(c).

46. *Ibid.* at ss. 4.6, 4.7.

47. *Ibid.* at sch. 1, cl. 4.3.4.

48. *Ibid.* at sch. 1, cl. 4.3.5.

Explicit consent is always required when the personal information is particularly sensitive, such as that in medical or financial records. Implied consent is appropriate when the information is less sensitive, a determination based on context. For example, subscription lists to certain special-interest magazines could be considered sensitive in nature.[49]

This approach is different from the European Data Protection Directive, which appears to offer broader consumer protection by asserting that European Union consumers must provide "unambiguous consent" prior to the collection of personal information.[50] As subsequently discussed, the European approach avoids the ambiguity surrounding the Canadian "reasonable person" approach and may better protect consumer privacy interests.

### *C. Governing the Watchers in an Era of Technology Change*

As discussed, technological changes have facilitated the ability of the private sector to watch and gather information about us. These changes, in part, motivated the passage of *PIPEDA* as a way to counter the perception that Canadians were losing their ability to keep certain aspects of their personal identity private.

In addition to Internet technologies, the private sector has begun employing a variety of other mechanisms that have privacy-encroaching implications.[51] These technologies include: (a) cell phones that report the precise geographic location of telephone calls; (b) smart cards used by supermarket chains that track details surrounding all purchases; (c) computer chips within consumer products that provide information

---

49. *Ibid.* at sch. 1, cl. 4.3.4 - 4.4.7.

50. The Directive permits the collection of information in certain circumstances without consumer consent. See *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 1995 O.J. L. 281, at art. 7.

51. For a discussion on the trend toward more powerful private sector surveillance technologies, see Ann Cavoukian & Don Tapscott, *Who Knows? Safeguarding Your Privacy in a Networked World* (Toronto: Random House, 1995); H. Jeff Smith, *Managing Privacy: Information Technology and Corporate America* (Chapel Hill: University of North Carolina Press, 1994).

on location and usage for inventory control purposes; (d) radio frequency identification tags in automobile tires that give information concerning car speed and location; (e) video or camera surveillance to deter crime; and (f) a variety of electronic monitoring techniques in the workplace to monitor phone calls and computer usage.

Similarly, government surveillance can be conducted with increasingly sophisticated technology. Writing in 1928 on the growing use of telephone wiretaps, Justice Brandeis recognized that technology could lead to more intrusive government search methods:

> Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[52]

In fact, technological developments such as satellite, cell phone and e-mail surveillance have made it easier for the government to watch us without being noticed.[53] The U.S. government has intensified its efforts to use more powerful emerging technologies to facilitate surveillance.[54] At some point, many of these different surveillance technologies could become integrated within large private sector and government databases. The state's ability to monitor, store, exchange, cross-index and retrieve digital information grows each year, allowing it to access potentially huge amounts of detailed personal information concerning individuals. While anti-terrorism laws have been subject to explicit evaluation prior to implementation, less attention has been paid to the technological developments that surround these policy changes. Technology can introduce significant social changes while escaping the "pattern of deliberation and review" that governs legal change.[55] The problem is

---

52. *Olmstead, supra* note 13 at 473.

53. For a discussion of emerging surveillance techniques, see Paul Kaihla, "Weapons of the Secret War" *Business 2.0* (November 2001) at 98, online: Business 2.0 <http://www.business2.com/articles/mag/0,1640,17511,FF.html>.

54. See the discussion in Part II C. below

55. For discussion, see Paul B. Thompson, "Justice, Human Rights and Ethics Issues in Science and Technology Policy" in Rigas Arvanitis, ed., "Science and Technology Policy", *Encyclopedia of Life Support Systems (EOLSS)* (Oxford: UNESCO, EOLSS Publishers, 2002), online: EOLSS <http://www.eolss.net>.

that inattention to technological developments leads to an increased risk of unanticipated adverse social outcomes.

## II. The New World: Weakened Legal Control Over Government Watchers

In the wake of the terrorist attacks, the Canadian government introduced legislation that would expand police and government surveillance powers to monitor or intercept communications.[56] The following analysis reviews how this legislation, in combination with technological developments, has diminished control over government surveillance in certain circumstances.[57]

### *A. Reduced Expectations of Privacy*

As discussed above, constitutional protections against government searches are based largely on reasonable expectations of privacy. Courts may grant greater latitude to government surveillance measures in light of the September 11th terrorist attacks because individuals have reduced privacy expectations in times of conflict or fear. As a result, individual privacy is sacrificed to promote greater collective security.[58] Further, if challenged, the Canadian federal government could argue that, in the context of domestic security concerns, broader surveillance powers are

56. For a comprehensive discussion of the main omnibus anti-terrorist legislation introduced by the Canadian government after September 11th, 2001, see Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-terrorism Bill* (Toronto: University of Toronto Press, 2001) [*Security of Freedom*].

57. For a review of the ways that the Canadian legislation affects privacy interests, see Lisa Austin, "Is Privacy a Casualty of the War on Terrorism?" in *ibid.* at 251 (asserting that the terrorism legislation is inconsistent with *Charter* values).

58. The passage by the Trudeau government of the *War Measures Act* in 1970 as a result of the FLQ crisis is instructive. Hundreds of individuals in Quebec were arrested without reasonable cause (although very few were ultimately convicted of any crime), which was considered an acceptable intrusion on privacy due to the threat of terrorism. These arrests took place prior to the enactment of the *Charter*, but were still subject to common law (and legislative) prohibitions against unreasonable search and seizure.

justifiable under section 1 of the *Charter* as a reasonable infringement on rights in a free and democratic society.

### *B. Reduced Judicial Scrutiny*

In some circumstances, Canadian legislation has reduced judicial scrutiny of government surveillance and other police powers. Similar developments have taken place in the United States.[59] In Canada, the surveillance powers in the *Criminal Code* were amended by the *Anti-terrorism Act*[60] to make it easier to use electronic surveillance against terrorist groups. This amendment eliminated the need to demonstrate that electronic surveillance will be used only as a last resort in an investigation of suspected terrorists. Further, the legislation extended the period of a wiretap authorization's validity from 60 days to up to one year when the police are investigating a terrorist group offence. The requirement to notify a target after surveillance has taken place can also be delayed for up to three years. Notably, a superior court judge must

---

59. The United States government has proposed a number of anti-terrorist measures that require weakened judicial oversight. Some of the measures involve enhanced airport and border security, while others are aimed at enhancing the ability of government to conduct surveillance of its own residents and residents in foreign countries. For example, the *Combating Terrorism Act*, passed by the U.S. Senate on September 13 2001, included provisions that increased the government's ability to monitor and seize data concerning e-mail messages and website visits (without resort to a court for a traditional search warrant). Under a lower threshold test whereby investigators need only establish that the sought-after information is relevant to an ongoing criminal investigation, the government will be able to access a list of an individual's e-mail destinations and traffic information (i.e. information contained in an e-mail's block header, the length of the message, whether any attachments were included, etc.) as well as a list of all websites visited. See *Combating Terrorism Act of 2001*, S.A. 1562 (2001). American legislation passed in the aftermath of September 11th additionally expanded government search powers by: (a) reducing probable cause standards; (b) limiting judicial review; and (c) creating a new "sneak and peak provision" that permits police to conduct searches without notifying suspects of the searches. See generally the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, Pub. L. No. 107-56, 15 Stat. 272, at ss. 206-225 [*USA PATRIOT Act*]. For discussion, see Marc Rotenberg, "Privacy and Secrecy after September 11" (2002) 86 Minn. L. Rev. 1115 at 1118.

60. R.S.C. 2001, c. 41 [*Anti-terrorism Act*]. This Act amended nineteen other laws, in addition to the *Criminal Code*, R.S.C. 1985, c. C-46 [*Criminal Code*].

still approve the use of electronic surveillance to ensure that these powers are used appropriately.[61]

The Canadian anti-terrorism legislation also expanded police search and arrest powers in the context of suspected terrorist activities. For example, a police officer who suspects on reasonable grounds that the detention of a person is necessary to prevent a terrorist activity may arrest and search that person without a warrant.[62] The Attorney General must consent to the arrest unless emergency conditions exist. Further, the detention after arrest must be judicially reviewed within 24 hours.

The investigative hearing provisions within the *Anti-terrorism Act* permit a police officer, for the purposes of a terrorism offence investigation, to apply *ex parte* to a judge for an order to gather relevant information.[63] The judge can then order the examination of a material witness who may possess such information. These preventative arrest and investigative hearing provisions are scheduled to sunset after five years unless the government takes steps to extend them.[64] According to one commentator:

> [T]he most dramatic impact of [the *Anti-terrorism Act*] is the creation of the sweeping substantive provisions designed to combat terrorism. Augmenting these substantive powers are a myriad of small changes that directly impact on liberty through detention or conditional restraint. Individually, most of these changes are small. Cumulatively, they claim significant liberty, in an insidious way.[65]

### *C. No Government Oversight*

Government accountability is eliminated for all intents and purposes when laws do not require any independent actor, such as a judge, to review government searches. In the wake of September 11th, Canada and

---

61. *Anti-terrorism Act*, *ibid.*, ss. 7-8.

62. *Ibid.*, s. 4, modifying s. 83.3 of the *Criminal Code*. The Solicitor General of Canada is required under s. 83.31(3) of the *Criminal Code* to prepare an annual report that sets out details surrounding the use of arrest without warrant.

63. *Ibid.*, s. 4, modifying s. 83.28 of the *Criminal Code*.

64. *Ibid.*, s. 4, modifying s. 83.32 of the *Criminal Code*.

65. See Gary T. Trotter, "The Anti-terrorism Bill and Preventative Restraints on Liberty" in *Security of Freedom*, *supra* note 56 at 246.

the United States broadened the powers of their intelligence services to monitor private communications. As an example of this trend, the *Anti-terrorism Act* granted the Minister of National Defence the power to authorize electronic surveillance of international communications without prior judicial authorization, while expanding the ability of Canadian intelligence agencies to monitor communications that potentially give rise to security risks.[66] The Minister must however be satisfied before issuing such authorization that measures exist to protect the privacy of Canadians. While this trend appears problematic, governments assert that public accountability over searches conducted by intelligence services can jeopardize investigations and place confidential sources at risk.

The proposed *Public Safety Act* would also expand police investigatory powers.[67] This legislation seeks to mandate the collection of personal information by airlines so that the information can be shared with the police, intelligence and government agencies.[68] For example, the legislation as initially proposed would have permitted intelligence agencies to examine passenger data, including information about flights within Canada, and order the police to make an arrest of any individual with an outstanding warrant, even if the warrant is completely unrelated to any terrorism offence. As a result of privacy concerns, this provision was deleted from the most recent version of the legislation.[69]

The proposed legislation would also increase the government's ability to share personal information on immigrants and refugees with other government agencies and foreign governments. In order to accomplish

---

66. See s. 102 of the *Anti-terrorism Act*. For discussion on the implications of the Canadian anti-terrorism legislation, see Don Stuart, "The Anti-terrorism Bill C-36: An Unnecessary Law and Order Quick Fix that Permanently Stains the Canadian Criminal Justice System" (2002) 14 N.J.C.L. 153.

67. See Canada Bill C-17, *Public Safety Act*, 2d Sess., 37th Parl., 2002 [*Public Safety Act*]. This Bill replaced two earlier bills as a result of sustained criticism by privacy advocates, among others.

68. Canadian Bar Association, News Release, "CBA Says Bill C-17 Poses Serious Threat to Privacy Rights of Canadians" (4 February 2003), online: Canadian Bar Association <http://www.cba.org/CBA/News/2003_Releases/2003-02-04_privacy.asp.>.

69. For discussion, see Privacy Commissioner of Canada's Appearance before the Legislative Committee on Bill C-17, *Public Safety Act*, Feb. 2002, online: Privacy Commissioner of Canada <http://www.privcom.gc.ca/media/02_05_a_030206_e.asp>.

this, the legislation proposes to amend the *Department of Citizenship and Immigration Act*[70] and the *Immigration and Refugee Protection Act*[71] to facilitate information gathering for security purposes. In particular, it would add a provision to the *Immigration and Refugee Protection Act* that would permit the promulgation of regulations relating to "the disclosure of information for the purposes of national security, the defence of Canada or the conduct of international affairs."[72]

In certain circumstances, changes to government information gathering processes and procedures have escaped the normal scrutiny that accompanies legislative proposals. For example, Canada and the United States have reached agreement on a border security plan that involves collecting and sharing information and intelligence on border crossers and other individuals.[73] Further, the Canada Customs and Revenue Agency has announced plans to retain information on air travellers entering Canada (discussed below in Part III).

### *D. The Promotion of New Surveillance Technologies*

In part, intelligence agents have been kept in check in the past due to a lack of resources: there were simply not enough technical, capital or human resources to scrutinize residents of their own countries. In the wake of September 11th, the Canadian and American governments have announced significant increases in their budgets for intelligence organizations, enabling them to expand their surveillance techniques to include the implementation of emerging technologies that can watch us without our knowledge or consent.[74]

Increased governmental use of technology to monitor the activities of Internet users is on the horizon. For example, the FBI has announced that it will increase the use of its DSC-1000 program (previously named

---

70. R.S.C. 1994, c. 31.

71. R.S.C. 2001, c. 27.

72. See *Public Safety Act*, *supra* note 67, part II, s. 150.1(1).

73. See DFAIT, *supra* note 6.

74. Privacy Commissioner of Canada, Annual Report to Parliament 2002-2003, online: Privacy Commissioner of Canada, <http://www.privcom.gc.ca/information/ar/02_04_08_e.asp>.

"Carnivore"), which permits investigators to sift through an Internet Service Provider's (ISP) e-mails. Due to the fact that Internet traffic originating in the United States is often routed by ISPs into Canada before crossing the border back to a U.S.-based destination, DSC-1000 is suspected to monitor Canadian web traffic and e-mails.[75]

Canadian legislators are similarly considering laws that would extend the reach of electronic surveillance mechanisms. For example, in June 2003, the Canadian government introduced Bill C-46, which would permit courts to order third parties such as ISPs to produce or prepare documents after finding that reasonable grounds exist to believe an offence has or will be committed.[76] While a DSC-1000 like program is not openly used by Canadian intelligence agencies, Canada participates along with the United States, New Zealand, the United Kingdom and Australia in a program called Echelon that permits investigators to monitor e-mails and chat room conversations. According to one report, 90% of Internet traffic is scanned by Echelon, which searches for words such as "heroin" or "child pornography" in order to focus investigators on suspected offenders.[77]

The Canadian Department of Justice has proposed that ISPs should grant police access to certain information on client use of Internet services.[78] For example, ISPs would be forced to maintain records on

---

75. Tyler Hamilton, "FBI Software Can Take Bite out of Canadians' Privacy" *Toronto Star* (25 March 2001), online: Creative Resistance <http://www.creativeresistance.ca/world-awareness/2001-march25-fbi-carnivore-software-takes-bite-out-of-canadian-privacy.htm>.

76. Bill C-46, *An Act to amend the Criminal Code (capital markets fraud and evidence-gathering)*, 2d Sess., 37th Parl., 2002, cl. 7 (adding s. 487.012 to the *Criminal Code*: "On the basis of an ex parte application containing information on oath that there are reasonable grounds to believe that an offence has been or is being committed, a court may order a person, other than a person under investigation for the offence, to produce or prepare documents within the time, at the place and in the form specified to a peace officer.")

77. See Ursula Sautter, "Electronic Surveillance: How the State can Spy on You", online: Time Europe Special Report <http://www.time.com/time/europe/webonly/tech/2000/07/privacy5.html>.

78. See Canada, Department of Justice *et al.*, *Lawful Access: Consultation Document* (Ottawa: Dept. of Justice, 2002) [*Lawful Access*]. For discussion, see Jason Young, "Surfing While Muslim: Privacy, Freedom of Speech and the Unintended Consequences of

their clients' "traffic data", which generally includes information such as website visits, e-mail destinations and any information concerning the routing of data information.[79] Under this proposal, to access this information, the police must obtain only a lower threshold production order that would not require a judge to find reasonable and probable cause that an offence had been or was being committed. According to the Canadian Association of Chiefs of Police, the threshold will be met if a judge "is satisfied . . . that the officer applying for the order is engaged in the *bona fide* execution of a lawful duty and the order is reasonably required in order for this duty to be carried out."[80] According to the Justice Department, the lower threshold production order is justified because it is less intrusive than a physical search of a suspect's premises.[81]

In an attempt to justify this lower threshold, data traffic information has been analogized to the information on the front of envelopes: the address, the stamp and the post date.[82] Accordingly, it is argued that police should be able to access traffic data under the same reduced legal thresholds that police face when they want to access mail as it travels through the post. The higher threshold requirement of obtaining a

---

Cybercrime Legislation", Centre for Innovation Law Student Working Paper (forthcoming in 2003, on file with author). The Canadian report was motivated in part by the perceived need to comply with the Council of Europe's Convention on Cybercrime, to which Canada is a signatory.

79. The Justice Department defines "telecommunications associated data" as "any data, including data pertaining to the telecommunications functions of dialing, routing, addressing or signaling that identifies, or purports to identify, the origin, the direction, the time, the duration or size as appropriate, the destination or termination of a telecommunication transmission generated or received by means of the telecommunications facility owned or operated by a service provider." See *Lawful Access*, *ibid.*

80. See Canadian Association of Chiefs of Police, "A Response to Government of Canada's Lawful Access Consultation Document" (Toronto: CACP, 2002), online: Canadian Association of Chiefs of Police <http://www.cacp.ca/english/download.asp?id=273>.

81. See *Lawful Access*, *supra* note 78 at 11.

82. See *e.g.* Robert Hubbard, Peter DeFreitas & Susan Magotiauz, "The Internet: Expectations of Privacy in a New Context" (2000) 45 Crim. L.Q. 170 (arguing that traffic data should not call for traditional protections against government searches).

search warrant is only necessary to access the contents of the envelope.[83] Similarly, it is argued that the proposed production orders would not permit the police to access the content of an e-mail. But traffic data, unlike the outside of an envelope, can offer a detailed view of personal identity once all of the elements of the data have been cross-referenced. Website visits, e-mail subject headers, attachment names, file types and sizes, and other information provide a potentially detailed record of individual identity. The envelope analogy is therefore inappropriate.

It would be more compelling to argue that individuals have a reasonable expectation that the police cannot access traffic data without first overcoming traditional hurdles such as obtaining a warrant prior to searching. This reasonable expectation is supported by the fact that ISP customers typically expect that ISPs will take reasonable steps to maintain the confidentiality of their online communications and will take measures to ensure that these communications remain secured against outside access.[84] The Privacy Commissioner and many public interest groups are concerned that measures such as Bill C-46 and the proposed production orders do not provide adequate privacy safeguards and increase the risk of abusive state surveillance practices.[85]

In addition to ISP monitoring, the FBI is reportedly developing a surveillance technology called "Magic Lantern," a computer program that can be installed remotely on the hard drive of a suspect's computer. Once installed, the program logs every keystroke made on the computer.[86] So even if a suspect deletes a potentially suspicious e-mail message prior to sending it, Magic Lantern could still log the message. This raises the danger of persecution, as the suspect could potentially be arrested for an Orwellian "thought crime."

---

83. *Ibid.*

84. See Ian Kerr, "The Legal Relationship between Online Service Providers and Users" (2001) 35 Can. Bus. L. J. 419 at 443.

85. See Privacy Commission, News Release (1 November 2002) online: Privacy Commissioner of Canada < http://www.privcom.gc.ca/media/nr-c/02_05_b_021101_e.asp >.

86. For discussion, see Christopher Woo & Miranda So, "The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance" (2002) 15:2 Harv. J. L. & Tech. 521.

The Pentagon has also proposed a project called Terrorism Information Awareness (the project's previous title, "Total Information Awareness", proved to be politically troublesome).[87] Under the proposed scheme, the U.S. government would gather vast amounts of information collected from the private sector. This information would then be combined into a vast database in an attempt to identify patterns associated with the planning of terrorist attacks.[88] For example, the U.S. government would seek to identify the purchase of plane tickets to designated countries, the purchase of materials that could be used for terrorist purposes, and payments for certain types of specialized training.[89] Further, the Terrorism Information Awareness project proposes to implement a host of emerging technologies to track terrorists. For example, the Department of Defense hopes to use "gait recognition" technologies to identify an individual by analyzing how he or she moves.[90]

The Canadian government is discussing the use of compulsory national identification cards, in part as a way to abate U.S. concerns surrounding border security.[91] These cards already exist in many countries, and are used to access public services such as health care and to prevent welfare fraud. They can be embedded with detailed information about an individual, and can be encoded with biometric identifiers (such as a digitized thumbprint). So-called "smart cards" store vast amounts of information, such as where an individual has traveled. The American Civil Liberties Union and other groups have opposed the use of such cards, in part because they could foster discrimination and harassment against minority groups and could be used as a tool to

---

87. See Defense Advanced Research Project Agency, *Report to Congress regarding the Terrorism Information Awareness Program*, online: Defense Advanced Research Projects Agency <http://www.darpa.mil/body/tia/TIA%20DI.pdf> [*Report to Congress regarding the Terrorism Information Awareness Program*].

88. *Ibid.* at 14-15.

89. *Ibid.*

90. *Ibid.* at A-19.

91. In November 2002, the Canadian government announced that it would begin to conduct hearings on the potential use of a national identification card system. See Justin Thompson, "National Identification Cards" (14 November 2002), online: CBC Online <http://www.cbc.ca/news/features/canadian_id.html>.

repress political dissent by tracking individuals who come from identifiable groups (such as Muslims).[92]

A concern has arisen that there will be increased video surveillance of public spaces such as airport or urban centers.[93] This type of surveillance is already prevalent in some parts of the world. According to one report, there are roughly 26 million surveillance cameras installed worldwide.[94] On average, a resident of London, England, is photographed or caught on video an astonishing three hundred times every day.[95]

Facial recognition technologies combined with video cameras pose the additional danger of racial profiling. Since the September 11th terrorists were of Middle Eastern origin, there is a greater chance that digital video surveillance will mistakenly identify someone from this group as a potential suspect, despite an absence of evidence concerning any wrongdoing.[96] Furthermore, computer surveillance technologies are not infallible, as code is programmed by human beings, who may have their own set of biases. As a result, these types of government searches might be challenged in Canada and the United States for violating constitutional protections surrounding the right to be free from discrimination on the basis of race, ethnicity or religion.[97]

Finally, it should be noted that governments are increasingly gathering information on our genetic identity. For example, the Canadian *Anti-*

---

92. See American Civil Liberties Union, "National Identification Cards", online: American Civil Liberties Union <http://archive.aclu.org/library/aaidcard.html>.

93. Charles Mandel, "Security Cams Not OK in Canada" *Wired News* (16 April 2002), online: Wired News <http://www.wired.com/news/politics/0,1283,51821,00.html>.

94. See Dan Farmer & Charles C. Mann, "Surveillance Nation", online: Technology Review <http:www.technologyreview.com/articles> (citing a report by J.P. Freeman).

95. *Ibid.* See Vito Pilieci "March Unveils Surveillance System" *The Ottawa Citizen* (28 September 2001) E1. Critics question the efficacy of the use of cameras to pursue security goals. See Clive Norris & Gary Armstrong, *The Unforgiving Eye: CCTV Surveillance in Public Space* (Hull: Centre for Criminal Justice Studies, 1997).

96. See *e.g.*, Kim Lunman, "Muslims 'Threatened' by New Law, Group Says" *The Globe and Mail* (15 May 2003) A7.

97. See *e.g.*, David Tanovich, "Using the Charter to Stop Racial Profiling: The Equality-Based Conceptions of Arbitrary Detention" (2002) 40 Osgoode Hall L. J. 145; Jeff Dominitz, "How Do Laws of Probability Constrain Legislative and Judicial Efforts to Stop Racial Profiling?" (2003) Am. L. and Econ. Rev. 412. For discussion of *Charter* issues and racial profiling, see *R. v. Brown* (2003), 64 O.R. (3d) 161 (C. A.).

*terrorism Act* extends the DNA warrant scheme and data bank to include terrorist offences in the list of "primary designated offences" for which DNA samples can be taken and stored.[98] Another example is provided by a recent high-profile homicide investigation in Toronto, in which the police canvassed surrounding neighborhoods and requested swabs from the cheeks of hundreds of residents to conduct DNA analysis.[99] Each individual's DNA was then checked against a databank to determine whether the individual could be a suspect.

### *E. Government Watchers and the Growing Surveillance Network*

At some point, information gained from public and private surveillance technologies could become integrated within large government databases. Many of the previously discussed initiatives, including the Department of Justice's proposal to access information collected by ISPs, the proposed national identification card system, and the Pentagon's proposed Terrorism Information Awareness program, would link government databases with private sector databases, and could create an environment where the right to be left alone was greatly diminished.[100] The ability to monitor, store, exchange and retrieve digital information grows each year, permitting state agents to access potentially dangerous levels of detailed and cross-indexed personal

---

98. As a primary designated offence, an order will be issued to obtain DNA samples for investigation purposes. *Supra* note 60, s. 17.

99. See CTV News Staff, "T.O. Police Defend Requesting DNA Samples", online: CTV <http://cfcnplus.ctv.ca/servlet/ArticleNews/scfcn/CTVNews/20030522/hollyjones_investigation_20030522/Canada/story>.

100. For a discussion of concerns surrounding government/business surveillance, including the issues of privatization, deregulation and joint ventures, see *e.g.* British Columbia, Information and Privacy Commissioner, *Annual Report 1998-99,* (Victoria: OIPC, 1998) at 13; Canada, Privacy Commissioner, *Annual Report 1995-96,* (Ottawa: Communication Group, 1996), online: Privacy Commissioner of Canada <http://www.privcom.gc.ca>; Canada, Privacy Commissioner, *Annual Report 1996-97,* (Ottawa: Communication Group, 1997), online: Privacy Commissioner of Canada <http://www.privcom.gc.ca>. See also Colin Bennett, "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" in Philip Agre & Marc Rotenberg, eds., *Technology and Privacy: The New Landscape* (Boston: MIT Press, 1997) 99 at 103.

information, such as website visits, e-mail records, health problems, credit history and credit card purchases, criminal records or interactions with the police, employment history, telephone records, TV viewing history, vacation destinations, etc.[101]

As David Lyon points out, "all modern societies are now heavily dependent on information infrastructures . . . Biometric, genetic and video data may now be processed and cross-checked against each other, by both state and commercial interests."[102] Under the guise of national interest, a government employee could scrutinize merged databases without the consent or even knowledge of the individual in question.

To a certain extent, *PIPEDA* works against the trend toward the sharing of information between state and industry actors. For example, it limits the collection and disclosure of personal information in many circumstances, which could reduce the amount of information at the disposal of state agents. Consider Internet service providers and the storage of traffic data. Under *PIPEDA*, they should only store this information as long as is necessary for business purposes. They may

---

101. On the implications of a government/business surveillance partnership, consider the following hypothetical example. TVcorp is a Toronto television cable station that provides cable services to consumers throughout Ontario, Quebec and upstate New York. TVcorp implements a monitoring technology that tracks the viewing habits of the subscribers to its digital cable services. The technology records every television program that is viewed, including the time spent watching it. TVcorp takes steps to aggregate this viewing information by geographic location, using postal codes. After deleting information that would identify individual consumers, the company sells a list of the recorded viewing habits to marketing companies who want to gauge audience demand for certain television shows. The RCMP obtains a warrant to attach a special computer console to TVcorp's main server. The software program scans the database of viewing records to locate individuals who have watched certain shows, such as a series of biographies on known terrorists. These viewers are cross-indexed against other viewing records that indicate which subscribers watched TV programs on fundamentalist religious practices. Armed with this knowledge, the RCMP begins to monitor the viewing habits of specific individuals. They are never told that this is occurring, and they may be unaware that such detailed surveillance is possible in the first place. If members of the public learn that government and industry *could* be tracking their viewing habits, it could potentially inhibit their viewing of "controversial" programming that does not conform to socio-political and sexual norms.

102. David Lyon, "Facing the Future: Seeking Ethics for Everyday Surveillance" (2001) 3 Ethics & Info. Tech. J. 171 at 172.

begin to delete previously archived information in order to comply with *PIPEDA* so that less information will be at risk of subsequent access by state agents.

Some might argue that the technologies themselves are neutral and that governments will simply decide one day to stop using them when the risk of terrorism declines. But technology is deterministic in nature because it shapes and changes the way we live. It is therefore unclear whether the clock can simply be turned back on the use of surveillance technologies. One view suggests that technological determinism depends in part on whether specific technologies are widespread and embedded within social structures. More embedded technologies are said to be more deterministic and resistant to change. As Thomas Hughes has commented, "[a] technological system can be both a cause and an effect; it can shape or be shaped by society. As they grow larger and more complex, systems tend to be more shaping of society and less shaped by it."[103] In other words, the Canadian government cannot "sunset" technologies in the same way it plans to "sunset" certain provisions of the anti-terrorism legislation. The infrastructure of social control may persist long after security concerns have abated. For these reasons, governments should take great care prior to implementing any additional surveillance technology.

# III. The Road Ahead: Watching the Watchers

In this Part, I will consider a few of the main policy concerns arising from the previously discussed legal and technological changes affecting government and private sector surveillance. Then I will propose a legislative and policy response.[104]

---

103. See Thomas P. Hughes, "Technological Momentum" in Merritt R. Smith & Leo Marx, eds., *Does Technology Drive History?: The Dilemma of Technological Determinism* (Cambridge: MIT Press, 1994) 112.

104. This Part does not attempt to comprehensively track many of the policy concerns surrounding privacy that have resulted from legislative changes in the post-September 11th environment. For example, the Canadian anti-terrorism legislation contains provisions that make it harder for some charities to raise money if they are connected with certain organizations located in foreign countries. Further, the legislation contains provisions

*A. The Watchers and the Erosion of Privacy*

There is extensive literature that scrutinizes the trend toward the use of increasingly powerful surveillance technologies and their potential social ramifications.[105] This literature suggests that technology can amplify the effect of legislative changes favouring surveillance practices. Two social ramifications of particular importance are: (i) repression of expression and (ii) stifling political dissent.

(i) The Repression of Expression

The growing use of surveillance technologies could ultimately endanger important democratic values, such as freedom of expression. Increased government and private sector surveillance, together with technological changes, leads to the risk that individuals will be increasingly watched by government agents without notice or consent. As our lives become increasingly tied to complex digital media technologies such as Personal Digital Assistants, digital television, personal computers, the Internet and cell phones, our actions and thoughts may become increasingly subjected to scrutiny by state agents.

---

that inhibit lawyer-client confidentiality in certain circumstances. In part, these provisions strive to impose positive duties on lawyers to provide client information to the government if they suspect terrorist activities or terrorist funding. Concerned lawyers throughout Canada have launched *Charter* challenges against many of these provisions. For commentary on similar efforts within the United States, see Marjorie Cohn, "The Evisceration of the Attorney-Client Privilege in the Wake of September 11" (2003) 71 Fordham L. Rev. 1233.

105. See Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Pantheon, 1977); David Lyon & Elia Zureik, "Privacy, and the New Technology" in David Lyon & Elia Zureik, eds., *Computers, Surveillance & Privacy* (Minneapolis: University of Minnesota Press, 1996); James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge: Harvard University Press, 1986); Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca, New York: Cornell University Press, 1992). Legal scholars who have discussed Foucault's conception of "panopticism" in the legal privacy and cyberspace context include Jack M. Balkin, "What is Postmodern Constitutionalism?" (1992) 90 Mich. L. Rev. 1966 at 1987, and Lawrence Lessig, "Reading the Constitution in Cyberspace" (1996) 45 Emory L. J. 869 at 895.

Digital records are potentially perfect, down to the minutest detail of every web site we visit, every e-mail we send and every keystroke we make. This creates a potentially permanent record of our activities and thoughts.

Governments and businesses have always watched us to a certain extent, but new surveillance technologies exponentially increase the ability of others to gather, store and index information about us. The nature of digital information and its accompanying distribution system facilitates the collection, exchange, manipulation and storage of information. Technology amplifies post-September 11th legal changes, increasing the risk that personal information will be accessed by state agents for reasons unrelated to national security. This growing surveillance network could effectively abolish the right to be left alone, a foundational right that, among other things, secures the freedom to express oneself. The Supreme Court of Canada has reflected on the importance of protecting a broad right to free expression:

> (1) seeking and attaining the truth is an inherently good activity; (2) participation in social and political decision-making is to be fostered and encouraged; and (3) the diversity in forms of individual self-fulfillment and human flourishing ought to be cultivated in an essentially tolerant, indeed welcoming, environment not only for the sake of those who convey a meaning, but also for the sake of those to whom it is conveyed.[106]

Greater scrutiny could make us take greater care before we visit a website or tap out a few thoughts on our word processors. If an individual thinks that her activities (website visits, television viewing, an impromptu "Singing in the Rain" dance in a downtown centre, etc.) will somehow be stored and potentially used against her in the future, she may change her behaviour and in so doing, edit her expression. Free citizens should have great latitude to express careless thoughts and words, to maintain diverse viewing habits and fantasies, and to express themselves in ways that harm nobody.

---

106. *Irwin Toy Ltd. v. Quebec (Attorney General)*, [1989] 1 S.C.R. 927 at para. 53.

(ii) Stifling Political Dissent

The ancient question "Who watches the watchers?" queries what political institutions are necessary to ensure that a government is held accountable for its actions. This question has only grown in importance in our era of significant technological changes, as government and private sector surveillance partnerships make it more difficult to hold state agents accountable for their actions.[107] Without strict government oversight, the private sector can amass personal information relating to identity, often without an individual's consent or knowledge. By tacitly allowing this process to go forward, the government creates the opportunity for future governments, under weakened legal restraints, to collect all of the detailed information they require.

Business and government surveillance that exclusively tracks terrorists is, of course, not the problem. The main problem is that surveillance could be turned against political dissenters, or other classes of vulnerable individuals, such as refugees, under the guise of national security. According to a report commissioned by the European Parliament's Civil Liberties Committee, states justify surveillance technologies under national interest rationales, but often use them to monitor political dissenters, journalists, minorities and political opponents.[108] The report concludes that surveillance technologies exert a powerful chilling effect on individuals who wish to dissent, and deter these individuals from exercising their democratic right to protest government policy. The potential for abusive state surveillance practices has been highlighted by

107. For discussion, see Eric Schmitt "Ashcroft Proposes Rules for Foreign Visitors" *The New York Times* (6 June 2002), online: The New York Times <http://www.nytimes.com/2002/06/06/politics/06VISA.html>; The Washington Post Staff "FBI Chief: 9/11 Surveillance Taxing Bureau" *The Washington Post* (6 June 2002), online: The Washington Post <http://www.washingtonpost.com/wp-dyn/articles/A2572-2002Jun5.html>; Hugh Winsor "Phillips Slew More Than Big Brother" *The Globe & Mail* (31 May 2000); Shawn McCarthy "Ottawa Pulls Plug on Big Brother Database: Canadians Promised Safeguards on Data" *The Globe & Mail* (30 May 2000); Andrew Mitrovica "RCMP, CSIS can access computer files on citizens" *The Globe & Mail* (19 May 2000) (on the federal government's Longitudinal Labour Force database, which was compiled with the cooperation of private sector sources).

108. Brian Rappert, "Assessing the Technologies of Political Control" (1999) 36 Journal of Peace Research, at 741.

a recent case where a police wiretap expert is suspected to have given misleading information to five Ontario judges in order to secure wiretaps in drug trafficking cases.[109] The disclosure so far has led to the dismissal of charges against and release of several accused individuals on the basis that the incriminating evidence was obtained illegally.

There is evidence that expanded investigatory powers have led some Canadian police and intelligence agencies to label certain groups as "terrorists" in order to justify the use of these powers.[110] Targeted groups have included Native Canadian activists, environmental and anti-globalization protesters, and anti-war activists.[111] Further, the expanded powers raise the risk of excessive racial profiling of certain minority groups, such as Muslims. The Canadian Islamic Congress indicates that hate crimes against Canadian Muslims have increased by more than 1,600% since September 2001, and reports "numerous cases" of warrantless interviews and interrogations of individuals of Muslim or Arab origin.[112] A report by the U.S. Inspector General is similarly critical of police practices in the months following the terrorist attacks, noting that there were "significant problems" in a number of cases where individuals were arrested and detained for lengthy periods despite having no connection to terrorist activities.[113]

There have been media reports that the Canadian government increasingly uses "security certificates" issued under the *Immigration and Refugee Protection Act*[114] in the aftermath of September 11th.[115] The

109. See Christie Blatchford "Fall of OPP's Wiretap Expert Could Set Off Judicial Storm" *Globe and Mail* (5 September 2003) A1.

110. For discussion, see "In the Shadow of the Law", *supra* note 7 at 2.

111. *Ibid.* The overbroad definition of "terrorist activities" within the *Anti-terrorism Act* may have contributed to these problems. See Kent Roach, "The New Terrorism Offences and the Criminal Law", in *Security of Freedom*, *supra* note 56 at 151 and 168. The final version of the legislation includes a provision which clarifies that political, religious or ideological beliefs will not be considered terrorist activities.

112. "In the Shadow of the Law", *supra* note 7 at 21.

113. See Office of the Inspector General, *The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks* (June 2003), online: United States Department of Justice <http://www.usdoj.gov/oig/special/03-06/index.htm>.

114. *Supra* note 71.

security certificate permits an individual to be arrested and detained without being charged with any immigration offence. Individuals can be deported once a judge validates the certificate based on information provided by the Canadian Security Intelligence Service (CSIS). According to a government spokesperson, the government has only issued 27 of these certificates since 1991 and courts have subsequently quashed only three.[116] Nevertheless, the Canadian Council for Refugees notes that recent changes to immigration laws heighten the risk that refugees will be denied permanent resident status because they now have fewer legal protections to counter allegations that they pose a security threat.[117]

*B. Policy Response: Watching the Watchers*

The tension between privacy and surveillance in the post-September 11th environment must be properly balanced. In this section, I will outline three ways that the law could address the concerns that arise from increased government and private sector surveillance in an era of rapid technological change.[118] The suggested approaches are designed to give individuals greater control over personal information that could be disclosed to the government and to ensure government accountability for its surveillance practices.[119]

---

115. See Andre Picard "WTO Protest Opens on Quiet Note" *Globe and Mail* (28 July 2003) A5. This article reports on protests directed at the policies of Immigration Canada.

116. Sue Bailey "Detainees' Relatives Demand Ottawa Act" *Toronto Star* (26 August 2003).

117. See Canadian Council for Refugees, *Refugees and Security* (February 2003), online: Canadian Council for Refugees <http://www.web.net/~ccr/security.PDF>.

118. For another perspective on how international law and legal institutions can promote national security in the post-September 11 environment, see Aaron Schwabach & Arthur Cockfield, "The Role of International Law and Institutions" in *Knowledge Base for Sustainable Development: An Insight into the Encyclopedia of Life Support Systems*, Volume III, (Oxford: UNESCO/EOLSS, 2002) at 611.

119. For another view on the need to promote public accountability, see Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy" (2002) 75 S. Cal. L. Rev. 1083.

(i) Strengthening Private Sector Surveillance Laws

The new federal privacy legislation, in the form of *PIPEDA,* is a welcome addition to the Canadian privacy law landscape.[120] The legislation strives to protect privacy while addressing the needs of the business community to efficiently collect data on customers in order to enhance service. It seems likely that information collected by the private sector will increasingly be placed at the disposal of government agents. In many circumstances, *PIPEDA* forces businesses to seek consent from consumers before disclosing sensitive personal information, enabling these consumers to have greater control over the information disclosed to other businesses and increasingly to government. In contrast, the U.S. approach, which combines self-regulation with the application of privacy laws to a few business sectors, offers greater room for the government to access private information without the knowledge or consent of individuals.

One limitation of *PIPEDA* lies in its consent provision. As discussed earlier, under *PIPEDA*'s "reasonable person" standard it will often remain unclear when a business must seek explicit rather than implicit consent from a customer prior to the collection, use or distribution of personal information.[121] For example, should information on website visits be considered sensitive personal information? If the answer is yes, an ISP likely has a legal duty to seek explicit consent prior to the permanent storage of this information. Without explicit consent, the ISP could only store this data on a temporary basis and delete it from its records when there was no longer a business reason for keeping it.

The answers to such questions will affect the Justice Department's recent proposal to force ISPs to collect and maintain information concerning website visits, since *PIPEDA* could frustrate this type of surveillance. However, the Department of Justice might argue that data on website visits is not particularly sensitive information, and that consumers implicitly consent to its permanent storage when they enter into a contract with the ISP.

120. *Supra* note 8. *PIPEDA* is discussed above, in Part II.

121. *Supra* note 8 at sch. 1, cl. 4.3.4.

It would be preferable to avoid ambiguity in *PIPEDA*'s consent provisions by mandating explicit consent prior to the collection or use of any personal information, as under the European Union approach that calls for "unambiguous consent."[122] The fact that governments increasingly tap into personal information held by the private sector suggests that individuals should be given a greater right to choose whether to disclose this information. Admittedly, it may be premature to suggest changes to *PIPEDA*, as the legislation and its consent provisions have yet to be explored in any detail by courts. However, if the consent provisions present the anticipated problems, legislative steps should be taken to address them.

(ii) Using a "Code Is Law" Approach to Watch the Watchers

In cyberlaw theory, it has been said that "code is law", insofar as code (the hardware and software technologies that enable the Internet) imposes constraints on the behaviour of Internet participants.[123] Legislators can pass laws to govern the code in order to achieve a policy goal. The Department of Justice's "Lawful Access" proposal represents an attempt to do just that, by requiring that ISPs use certain technologies to facilitate the tracking of online information by the police.[124]

The Canadian government should consider passing legislation to govern how state agents use code to collect and store personal information.[125] Certain forms of particularly sensitive information could

122. *Supra* note 50.

123. See generally Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) at 6. For example, law could mandate that all public libraries install software filters so minors cannot access pornography.

124. *Lawful Access*, *supra* note 78.

125. For discussion of the need to employ built-in operational safeguards to reduce potential abuse, see *Report to Congress regarding the Terrorism Information Awareness Program*, *supra* note 87 at 33-35. These safeguards could include: (a) ongoing testing of the efficacy and accuracy of search tools and oversight of research and development of surveillance technologies; (b) implementing security measures to protect against unauthorized access; (c) legal review prior to the use of surveillance technologies; and (d) spot auditing of surveillance technologies.

be stored in files that require independent judicial authorization for access.[126] For large databases, code could allow personally identifying information to be "scrubbed" from search results delivered to government analysts, thereby mediating the tension between security and privacy.[127] Analysts could then scan these scrubbed search results to detect patterns of behaviour that gave rise to security concerns without infringing on privacy rights. Any subsequent investigation could then focus on individuals whose identities would be revealed after authorities complied with traditional legal safeguards, such as obtaining a search warrant. This system would permit the collection and aggregation of large quantities of data for sound public policy reasons without maintaining permanent records that disclose individual identity.

The law should also mandate the tracking of information on database searches performed by government agents. By requiring code that logs searches made by government personnel, authorities and wrongly-accused individuals will have access to an audit trail that can assist them in determining whether the surveillance was legally permissible in the first place.[128] The record would also permit authorities and citizens to correct errors in information obtained through surveillance. Further, the mere fact that searchers will be aware that their computer usage is being recorded will deter abusive surveillance practices.

This approach has been adopted to a certain extent in a recent federal government initiative. As touched on earlier, the Canada Customs and Revenue Agency proposed to create an air traveler database that would retain information for a period of six years. As a result of sustained criticism by public interest groups and the former Privacy Commissioner, the plan was modified in March 2003. Proposed changes

126. For discussion, see Dan Farmer & Charles C. Mann, "Surveillance Nation-Part Two", online: Technology Review <http://www.technologyreview.com/articles> (discussing how the Malaysian government is implementing smart cards with embedded software that encrypts and compartmentalizes personal information to ensure that government or business can access only certain types of information).

127. For discussion, see Leslie Walker "Balancing Data Needs and Privacy", *Washington Post* (8 May 2003), online: The Washington Post <http://www.washingtonpost.com/ac2/wp-dyn/A25316-003May7?language=printer>.

128. *Ibid.* The audit log can be encrypted and stored in fragments with independent organizations to prevent tampering and protect its integrity.

include: permitting access to this information by customs officials for 72 hours after the flight, then restricting access; restricting access to a limited number of intelligence officials; purging information not required for customs purposes (such as what travelers ordered to eat); and requiring that police get a warrant unless exigent circumstances exist.

(iii) Watching the Watchers Through Enhanced Reporting

The public should be entitled to review the impact of legislative changes that deal with police practices and investigations. Under the *Anti-terrorism Act*, the Attorney General and Solicitor General of Canada, as well as the provincial Attorneys General and Ministers responsible for policing, will be required to report annually to Parliament on the use of preventive arrest and investigative hearing provisions. Further, a Parliamentary review of the anti-terrorism legislation as a whole is scheduled to take place in 2004.[129] It may however be necessary to have a more focused review of police use of emerging technologies for surveillance and investigations. The government should strike an independent committee to oversee these changes to prevent abusive state practices. Similarly, it has been suggested that the Legislative Committee on Bill C-17 (the *Public Safety Act*) could be converted into a Special Committee with responsibility for overseeing all anti-terrorism laws, and that the Standing Committee on Justice and Human Rights should participate in such oversight.[130]

This independent oversight mechanism could be combined with recent efforts by the Canadian government to make federal agencies more sensitive to policies that encroach on privacy. In May 2002, the Canadian government mandated through its Privacy Impact Assessment Policy that every federal program and service will undergo a Privacy Impact Assessment (PIA).[131] The PIA involves the preparation of a

129. See *Anti-terrorism Act*, *supra* note 60, at s. 145.

130. See In The Shadow of the Law, *supra* note 7 at 2.

131. See Treasury Board of Canada Secretariat, "Privacy Impact Assessment Policy", online: Treasury Board of Canada Secretariat <http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp>.

report that ensures privacy is protected when an existing or new policy is implemented. The Office of the Privacy Commission is charged with reviewing the PIAs. Further, the Office of the Information Commissioner provides reports on the privacy policies of several federal agencies along with statistics concerning response rates to access to information requests.[132] These encouraging efforts should be broadened into an independent examination of the impact of anti-terrorism legislation on privacy rights and interests.

Accountability should also be increased by ensuring that the government follows its own guidelines on the disclosure of information concerning police investigations. Currently, section 195 of the *Criminal Code* requires the Solicitor-General to publish an annual report on authorizations granted for the interception of private communications. The government has failed to fulfill this obligation in the last two years, ostensibly due to delays in accessing the data collected by police forces.[133]

In 2003, the Solicitor-General published its annual report for 2001, which covers roughly the four-month period following the terrorist attacks. In 2001, 121 authorizations were granted to monitor private communications. This is lower than the number granted in each of the previous four years.[134]

According to the report, the majority of the 2001 authorizations were granted to pursue suspected drug trafficking and related crimes. Only three authorizations that might be tied to potential terrorist activities were granted for alleged violations of the *Immigration Act*. The most frequently used method of intercepting private communications was the use of "telecommunication", which presumably means a traditional

---

132. See *e.g.* Privacy Commissioner, "Special Report to Parliament by the Information Privacy Commissioner: Compliance with Response Deadlines", online: Privacy Commissioner of Canada <http://www.privcom.gc.ca/information/ar/02_04_10_02_e.asp>.

133. See Tyler Hamilton "Powers Snoop More, Disclose Less," *The Toronto Star* (24 March 2003), online: The Toronto Star <http://www.thestar.com>.

134. For example, 150 authorizations were granted in 2000 and 154 authorizations were granted in 2001. See Solicitor General of Canada, *Annual Report on the Use of Electronic Surveillance 2001*, online: Solicitor General of Canada <http://www.sgc.gc.ca/Publications/Policing/Electronic_Surveillance_2001_e.asp>.

wiretap rather than Internet surveillance. The report, however, does not provide details with respect to any searches that used emerging technologies. It would be helpful to provide this information in order to abet concerns surrounding the use of more powerful surveillance technologies. Greater public confidence could be promoted through an indication that these technologies have not yet been deployed, if that is the case.

Other reports have also been remarkably brief. For example, the Justice Department has provided its first annual report on the use of preventative arrests and investigative hearings from December 24, 2001 to December 23, 2002.[135] The report notes that the police did not exercise either power during this period. However, a civil liberties organization notes that the report "provided scant information on the use of merely two articles of the Act. It is too restrictive and limited in scope to offer a clear and just appreciation of the impact of the measures adopted (or still being considered) by Parliament since September 11th , 2001."[136]

Public accountability for surveillance practices can also be bolstered through additional law reform efforts. The federal *Privacy Act*, which governs public sector collection practices, must be amended to ensure that government agents follow fair and comprehensive information collection practices and guidelines, such as those set out in *PIPEDA*.[137] The Privacy Commissioner has reviewed the *Privacy Act* in recent years and recommended over one hundred changes to improve it and make it

---

135. See Canada, Department of Justice, *Annual Report concerning Investigative Hearings and Recognizance with Conditions: December 24, 2001—December 23, 2002* (Ottawa: Department of Justice, 2003), online: The Department of Justice < http://canada.justice.gc.ca/en/terrorism/annualreport.html >.

136. See In the Shadow of the Law, *supra* note 7 at 1.

137. See OECD, Department of Science, Technology & Industry, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Doc. No. OCDE/C(80)58 (1980); Canadian Standards Association, "Model Code for the Protection of Personal Information", CAN/CSA-Q830 (1995). See also Flaherty, *supra* note 32 for a discussion of the importance of fair information practices in understanding the development of information privacy law, even though specific conceptions of the principles vary.

more responsive to current concerns.[138] The *Privacy Act* was passed several decades before *PIPEDA* and does not reflect the same comprehensive approach to ensuring the integrity of collection, use and distribution of personal information. This approach is achieved in *PIPEDA* by: (a) ensuring that there are no secret information gathering practices; (b) ensuring that individuals can find out what information about them has been collected and how it has been used; (c) ensuring that individuals can prevent the state from using information for a purpose other than that for which it was collected; (d) ensuring that individuals can amend incorrect information that has been collected; and (e) ensuring that the collected data is maintained in a secure area where it cannot be misused or tampered with.

Similarly, the *Access to Information Act*[139] should be reviewed in order to ensure individual access to information on police searches and investigations in certain circumstances. A government taskforce in 2002 recommended 139 changes to access to information legislation to ensure that Canadians can properly access information held by government agencies.[140] The *Anti-terrorism Act* modified provisions in the *Access to Information Act* to a certain extent, although the final version of the legislation still permits individuals to apply to the Federal Court of Appeal to have a security certificate varied or cancelled.[141]

The most problematic issues of accountability arise when the government need not disclose information concerning its surveillance practices. Under the guise of public interest, the state can withhold

---

138. Privacy Commissioner of Canada, "Annual Report (1998-1999)", online: Privacy Commissioner of Canada, <http://www.privcom.gc.ca/information/ar/02_04_08_e.asp>.

139 R.S.C. 1985, c. A-1.

140. Canada, *Report of the Access to Information Task Force, Access to Information: Making it Work for Canadians*, online: Access to Information Review Task Force <http://www.atirtf-geai.gc.ca/report2002-e.html>.

141. See the *Canada Evidence Act* R.S.C. 1985, C-5, s. 8.131 [*Evidence Act*]; *Anti-terrorism Act*, s. 87. The first reading of the terrorism legislation contained significantly broader powers to the Attorney General to prevent disclosure, but the provisions were subject to sustained criticism by some commentators. See *e.g.* George Radwanski, *Testimony Regarding Bill C-36, the Anti-terrorism Act, to the House of Commons Standing Committee on Justice and Human Rights*, online: The Privacy Commissioner of Canada <http://www.privcom.gc.ca/speech/02_05_a_011024_e.asp>.

access to such information. Pursuant to the *Canada Evidence Act*, the Attorney General of Canada can personally issue a certificate prohibiting the disclosure of information to protect international relations, national defence, or national security.[142] Such withholding may be subject to legal appeal, but this route may be effectively closed to the extent that individuals do not have the resources to pursue an appeal. In any event, targets of government surveillance will often be unaware of the surveillance unless charges are laid against them.

For these reasons, some commentators have argued that the law should narrowly circumscribe the areas in which national security can be used to justify non-disclosure.[143] However, with recent legal changes broadening the police powers that relate to the maintenance of national security, the only hope may be to wait for an improved political climate and a return to more effective restrictions on discretionary police surveillance.

# Conclusion

As a result of the tragic terrorist attacks of September 11th, 2001, legal protections surrounding government surveillance have been reduced, due to the prevailing view that privacy must be sacrificed in order to benefit from enhanced security. Further, technological developments are permitting government actors to expand their surveillance powers significantly, in part by tapping into detailed information collected by the private sector. Technology can act as a kind of amplifier, allowing well-meaning but intrusive monitoring by both the private sector and government to inhibit critical values such as freedom of expression and the right to privacy. A lack of public accountability for such surveillance increases the risk of abusive police actions.

To address these concerns, laws that govern private sector information gathering should be strengthened. They must mandate technological measures to ensure that personal information is segregated and secured

142. See *Evidence Act, ibid.* at s. 38.13.

143. See *e.g.*, Stuart, *supra* note 66 at 158-162 (arguing that the Canadian anti-terrorism laws have "put into our permanent laws a huge and complex web of dragnet and extraordinary police and C.S.I.S. powers").

within large databases, and they must increase public oversight of the use of technology in state surveillance.

Unless measures are taken to properly manage the evolving tension between security, privacy and technology, the institutionalization of private sector and government surveillance practices risks creating a citizenry that is increasingly complacent about such scrutiny. Pervasive scrutiny by unseen forces may one day become the norm. We could become so undemocratic that we cease to review potentially abusive state actions. In other words, we may fail to ask: Who is watching us? Who is monitoring, tracking, compiling, editing, sorting and distributing information about us? *Sed quis custodiet ipso custodes*—who watches the watchers?