The State of Privacy Laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government

Arthur J. Cockfield*

* Assistant Professor, Queen's University Faculty of Law. This article draws from and updates an earlier article. See Arthur J. Cockfield, "Who Watches the Watchers?: A Law and Technology Perspective on Government and Private Sector Surveillance" (2003) 29 Queen's L. J. 364. An earlier draft of this paper was presented at the Comparative IP and Cyberlaw Symposium at the University of Ottawa on October 4, 2003.

The State of Privacy Laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government

Arthur J. Cockfield

INTRODUCTION

IN THE WAKE OF THE TRAGIC EVENTS of September 11, 2001 the Canadian government changed laws to facilitate the surveillance of residents, citizens and foreign individuals. Many continue to be concerned that legal and technology developments could serve to undermine privacy rights and interests, potentially leading to racial profiling and the inhibition of political dissent and freedom of expression.[1]

The purpose of this article is to offer a tentative evaluation of the Canadian government's efforts in this regard. A review of government practices suggests that state agents are not generally subjecting Canadians to overly intrusive surveillance practices, although select areas of potentially abusive state actions have become known. The article concludes by giving the Canadian government a C+ for its surveillance practices and use of privacy-encroaching technologies of surveillance. To obtain better grades, the government should develop more public accountability mechanisms, such as an independent oversight committee to monitor potential abuses.

Part 1 provides an overview of the legal and technological changes surrounding government and private sector surveillance. An understanding of the legal regime governing industry information collection practices is necessary because governments are increasingly tapping into databases of personal information previously collected by businesses. This Part ends by discussing the relationship between privacy law and technology. Part 2 sets out empirical and anecdotal evidence concerning Canadian government surveillance practices and

1. Throughout this article, the term "privacy" is meant to signify the ability of an individual to control what information about personal identity she wishes to let others know. The right to privacy is a right that is protected by some law or norm. The definition of privacy is somewhat contentious and commentators have come up with more expansive and more narrow definitions than this one. The emphasis on control over personal information is closer to the notion of "information privacy." 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.

the use of expanded police powers to counter terrorist activities. There are limited available data about these practices, although two government reports suggest that state agents have not significantly increased the amount of surveillance or used new powers of preventative arrest or investigative hearings. Certain reports, however, have noted cases involving possible racial profiling of Canadian residents.

*

1. LEGAL AND TECHNOLOGICAL CHANGES AFTER SEPTEMBER 11

THIS SECTION BRIEFLY SETS out some of the main changes to laws that govern government and industry surveillance that have been made in the last two years.[2] The review also focuses on technology developments that have accompanied these changes and concludes by discussing the relationship between these technologies and privacy laws.

1.1. Government Surveillance

1.1.1. Legal Reform of Laws that Regulate Privacy

In Canada, the surveillance powers in the *Criminal Code* have been amended in 2001 by the *Anti-Terrorism Act* to make it easier to use electronic surveillance against terrorist groups.[3] The need to demonstrate that electronic surveillance is a last resort in the investigation of terrorists has been eliminated. Further, the legislation has extended the period of validity of a wiretap authorization from the previous 60 days to up to one year if the police are investigating a terrorism group offence. The requirement to notify a target after surveillance has taken place can also be delayed for up to three years. A Superior Court judge will still have to approve the use of electronic surveillance to ensure that these powers are used appropriately, however.

Canada's 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 this person without a warrant.[4] The Attorney General must consent to the arrest unless certain emergency conditions exist. Further, the detention after arrest must be reviewed judicially within twenty-four hours.

The investigative hearing provisions within the *Act* permit a police officer, for purposes of investigating a terrorism offence, to apply *ex parte* to a judge for an order to gather information relevant to that investigation. The judge

---

2. Federal and provincial laws that affect privacy interests are extensive and complex. The review attempts only to touch on some of the main recent developments.

3. See *Anti-Terrorism Act*, S.C. 2001, c.41. <http://laws.justice.gc.ca/en/A-11.7/index.html>. 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 Ronald Daniels, Patrick Macklem & Kent Roach eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press, 2001) at 251. (Arguing that the terrorism legislation is inconsistent with *Charter* values).

4. *Criminal Code*, R.S.C. 1985, c. C-46, s.83 .3 (4). <http://laws.justice.gc.ca/en/C-46/index.html>. The Solicitor General of Canada is required under subsection 83.31 (3) of the *Criminal Code* to prepare an annual report that sets out details surrounding the use of this section on arrest without warrant.

may order the examination of a material witness who may possess information concerning a terrorism offence that has been or may be committed. The preventative arrest and investigative hearing provisions are scheduled to sunset after five years unless the government takes steps to extend them.

The *Act* amended nineteen other laws in addition to the *Criminal Code*. According to one commentator, "The 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 myriad small changes that directly affect liberty through detention or conditional restraint. Individually, most of these changes are small. Cumulatively, they claim significant liberty, in an insidious way."[5]

In some circumstances, the *Act* abolished traditional Common Law safeguards that require independent judicial authorization prior to the issuance of a search warrant. For example, the *Anti-Terrorism Act* granted the Minister of National Defence the power to authorize electronic surveillance of international communications without the need to seek prior judicial authorization, and expanded the ability of Canadian intelligence agencies to monitor communications that potentially give rise to security risks.[6] The Minister, however, must be satisfied before issuing such authorizations those measures are in place to protect the privacy of Canadians.

Pursuant to the *Canada Evidence Act*, the Attorney General of Canada may personally issue a certificate prohibiting the disclosure of information to protect international relations, national defence or national security.[7] The *Anti-Terrorism Act* modified provisions in the *Access to Information Act*[8] to a certain extent, although the final version of the legislation permits individuals to continue to apply to the Federal Court of Appeal to have the certificate varied or cancelled.[9]

A proposed *Public Safety Act* would also expand police powers of investigation in certain circumstances.[10] This proposed legislation seeks to mandate the collection of personal information by airlines so that the information may be shared with the police, and intelligence and government agencies.[11] Initially, the legislation would have permitted intelligence agencies to examine passenger data, including information on flights within Canada, and notify the police to make

---

5. See Gary T. Trotter, "The Anti-Terrorism Bill and Preventative Restraints on Liberty" in *The Security of Freedom*, *supra* note 3 at 239, 246.
6. See s.102 of the *Anti-Terrorism Act*, *supra* note 3. For a discussion of 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.
7. *Canada Evidence Act*, R.S.C. 1985, c. C-5, s. 38.13, <http://laws.justice.gc.ca/en/C-5/index.html>.
8. *Access to Information Act*, R.S.C. 1985, c. A-1, <http://laws.justice.gc.ca/en/A-1/index.html>.
9. *Supra* note 7 at s. 38.131 of the *Canada Evidence Act*; s. 87 of the *Anti-Terrorism Act*, *supra* note 3. 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.* Canada, House of Commons, The Anti-Terrorism Act, Standing Committee on Justice and Human Rights, George Radwanski, Testimony Regarding Bill C-36 (23 October 2001). The final version of the bill also indicates that the certificate can be issued only after an order or decision for disclosure has been made in a proceeding.
10. See Canada, Bill C-17, *Public Safety Act 2002*, 2d Sess., 37th Parl., 2002 (First reading, 31 October 2002). This Bill replaced two earlier bills as a result of sustained criticism by privacy advocates, among others.
11. See Canadian Bar Association Press Release "CBA Says Bill C-17 poses Serious Threat to Privacy Rights of Canadians" (4 February 2003), <http://www.cba.org/cba/News/2003_Releases/PrintHtml.asp?DocId=51371>.

an arrest of any individual with an outstanding warrant, even if the warrant were completely unrelated to any terrorism offence. As a result of privacy concerns, this provision was deleted from the most recent version of the legislation.[12]

The proposed legislation would also increase the government's ability to share personal information regarding immigrants and refugees with other government agencies or foreign governments. To accomplish this goal, the legislation proposes to amend the *Department of Citizenship and Immigration Act*[13] and the *Immigration and Refugee Protection Act*[14] to facilitate information gathering for security purposes. In particular, the legislation would add a provision to the *Immigration and Refugee Protection Act* that would permit the promulgation of regulations relating to "the disclos[ur]e of information for the purposes of national security, the defence of Canada or the conduct of international affairs."[15]

In certain circumstances, changes to government information-gathering processes and procedures have escaped the normal scrutiny that accompanies legislative proposals. For example, in December 2001, Canada and the United States reached agreement on a border security plan that involves collecting and sharing information and intelligence on individuals who cross the border and other individuals.[16] Further, the Canada Customs and Revenue Agency (CCRA) announced plans to retain information on air travelers entering Canada (discussed below in Part 2).

1.1.2. Technology Developments

Technological innovations and developments have accompanied legal reforms surrounding government surveillance. This section briefly explores how the Canadian and United States governments are implementing or planning to implement technologies that facilitate surveillance. The discussion of United States developments takes place for two reasons. First, Canadian regulators, at times, pursue a strategy of regulatory emulation whereby they implement laws, policies and technologies that match those in the United States to ensure that cross-border economic flows are not disrupted (as occurred under the "Smart Border" plan).[17] Second, the United States technologies of surveillance might be used to gather information on Canadian citizens and residents. A Canadian civil liberties group has warned that "[w]e could soon find ourselves in a situation where all personal information on Canadians will be in the hands of, and man-

12. For discussion of concerns surrounding the *Public Safety Act*, see Privacy Commissioner of Canada, Testimony, "Privacy Commissioner of Canada's Appearance before the Legislative Committee on Bill C-17, Public Safety Act," (6 February 2003), <http://www.privcom.gc.ca/media/02_05_a_030206_e.asp>.

13. *Department of Citizenship and Immigration Act*, S.C. 1994, c. 31, <http://laws.justice.gc.ca/en/C-29.4/index.html>.

14. *Immigration and Refugee Protection Act*, S.C. 2001, c. 27, <http://laws.justice.gc.ca/en/I-2.5/index.html>.

15. See *Public Safety Act*, *supra* note 10 at Part 11, cl. 150.1 (1).

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

17. On Smart Border, see *ibid*. 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.

aged centrally by American securities agencies unaccountable to Canadian Parliament and the Canadian public."[18]

The Canadian Department of Justice has proposed that Internet Service Providers "ISPs" grant police access to certain information on their client's use of internet services.[19] For example, ISPs would be forced to maintain records on their clients' "traffic data," which generally includes information such as web site visits, the destination of emails or any information concerning the routing information.[20]

Under the proposal, the police would seek only a lower threshold "production order" that did not require an independent judge to find reasonable and probable cause that an offence had been or was being committed.[21] 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."[22] The lower threshold production order is justified, according to the Department of Justice, because the order is less intrusive than a physical search of a suspect's premises.[23]

In June 2003, the Canadian government introduced legislation that 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.[24] The former federal Privacy Commissioner and many public interest groups were concerned that the proposals do not have adequate privacy safeguards, increasing the risk of abusive state surveillance practices.[25]

In addition to monitoring ISP data traffic, an increased use of technologies that monitor the activities of Internet users appears to be on the horizon. The FBI has announced that it will increase the use of its DSC 1000 program (previously named "Carnivore"), which permits investigators to sift through an ISP's

---

18. *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)* (May 2003) at 4, reprinted in Canadian Association of University Teachers Bulletin No. 6 [hereinafter *In the Shadow of the Law*], <http://www.interpares.ca/en/publications/pdf/shadow_of_the_law.pdf>.

19. See Canada, Department of Justice *et al.*, *Lawful Access: Consultation Document* (Ottawa: Department of Justice, 2002) [*LawfulAccess*]. For discussion see Jason Young, "Surfing While Muslim: Privacy, Freedom of Speech and Unintended Consequences of Cybercrime Legislation" McGill L.J. (forthcoming). 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 but has not passed as legislation.

20. Lawful Access, *ibid.* The Department of Justice 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."

21. *Lawful Access*, *ibid* at 11.

22. Canadian Association of Chiefs of Police, Response to Government of Canada's Lawful Access Consultation Document (Toronto, 16 December 2002) at 18 of the PDF file, <http://www.cacp.ca/english/library/download.asp?ID=274>.

23. See *Lawful Access*, *supra* note 19 at 11.

24. Bill C-46, *An Act to amend the Criminal Code* (amdt.—capital markets fraud and evidence-gathering), 2d Sess., 37th Parl., 2002, cl. 7 (First reading, 12 June 2003) (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.)

25. Canada, Parliament, Sub-Committee on National Security of the Standing Committee on Justice and Human Rights, Privacy Commissioner of Canada's Appearance, (10 February 2003), at 1535, <http://www.parl.gc.ca/InfoComDoc/37/2/SNAS/Meetings/Evidence/SNASEV02-E.HTM>.

emails. Due to the global nature of the internet and the fact that internet data traffic originating in the United States is often routed by ISPs into Canada before crossing the border again to arrive at a United States-based destination, some suspect that Carnivore monitors Canadian web traffic and emails.[26]

Canadian legislators are similarly considering laws to extend the reach of electronic surveillance mechanisms. Although the Canadian Security Intelligence Service (CSIS) and other branches of the government do not (openly) use a Carnivore-like program, Canada participates in a program called Echelon—along with the United States, New Zealand, the United Kingdom and Australia—that permits investigators to monitor emails or 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 their targets.[27]

In addition to ISP monitoring, the FBI is reportedly developing a surveillance technology called "Magic Lantern" that is essentially a computer program that can be installed remotely on the hard drive of a suspect's computer; once installed, the program logs all keystrokes on the computer.[28] Accordingly, even if the suspect deletes a potentially suspicious email message before sending it, the FBI would still log the message. This raises the prospect of prosecution, as the suspect could potentially be arrested for an Orwellian "thought crime."

Finally, the Pentagon has proposed the development of a project called Terrorism Information Awareness (the project previously carried the politically more troublesome name of Total Information Awareness).[29] Under the proposed scheme, the U.S. government would first gather vast amounts of information collected from the private sector. Next, this information would be combined into a vast database that tried to identify patterns associated with planning terrorism attacks.[30] 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 terrorism purposes or payments for certain types of specialized training.[31] Further, the Terrorism Information Awareness project proposes to implement a host of emerging technologies to track terrorists. Through "gait recognition" technologies, for example, the Department of Defense hopes to be able to identify an individual by analyzing how he or she moves and walks.[32]

The Canadian government is discussing the use of compulsory national identification cards, in part as a way to abate United States concerns surrounding

---

26. Tyler Hamilton, "FBI Software Can Take a Bite out of Canadians' Privacy" *Toronto Star* (25 March 2001) B1.
27. See Ursula Sautter, "Electronic Surveillance: How the State Can Spy On You" *Time.com* (28 July 2000), <http://www.time.com/time/europe/webonly/tech/2000/07/privacy5.html>.
28. For discussion, see Christopher Woo and Miranda So, "The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance" (2002) 15 Harv. J. L. & Tech. 521.
29. See Defense Advanced Research Project Agency, In response to Consolidated Appropriations Resolution: Report to Congress Regarding the Terrorism Information Awareness Program (20 May 2003) Pub. L. No. 108-7, Division, §§ 111 (b). The Senate cut funding in the Fall of 2003 to TIA although aspects of the program continue in other Pentagon divisions. See William Webb and Eli Lehrer, Give Awareness a Chance, *National Review Online* (15 October 2003), <http://www.nationalreview.com/comment/webb-lehrer200310150826.asp> (arguing that TIA would be a useful weapon in the war against terrorism).
30. *Ibid.* at 14–15.
31. *Ibid.* at 14.
32. *Ibid.* at A–19.

border security.[33] These cards already exist in many countries and are used to access public services such as health care, or to prevent welfare fraud. They can be embedded with detailed information concerning an individual using biometrics (*e.g.*, a digitized thumbprint embedded in the card). So-called "smart cards" have built-in microchips that can store vast amounts of information, such as where an individual has traveled as well as their medical history. The American Civil Liberties Union (ACLU) and other groups have opposed the use of national identification cards, in part because they can foster discrimination and harassment against minority groups and could be used as a tool to repress political dissent.[34]

Additional proposals have included a call for increased video surveillance of public spaces such as airports or urban centers. Digital video surveillance scans an individual's face in order to compare it to a database of suspects. This type of surveillance is already prevalent in some parts of the world: according to one report, there are roughly twenty-six million surveillance cameras installed throughout the world.[35] Residents in the city of London, are on average, photographed or caught on video an astonishing three hundred times daily.[36]

When combined with video cameras, facial recognition technologies pose an additional danger of racial profiling. As the September 11th terrorists were of Middle Eastern origin, the chances that someone from this identifiable group will be mistaken by digital video surveillance as a potential suspect increases. In other words, people from an identifiable group will be monitored more closely than others, despite an absence of evidence concerning any individual wrongdoing.[37] Computer surveillance technologies are fallible: code is programmed by human beings under the direction of other human beings, possibly with their own set of biases. These types of government searches might be challenged in Canada and the United States under constitutional protections surrounding the right to be free from discrimination based on race, ethnicity or religion.[38]

Finally, governments are increasingly gathering information on our genetic identity. After a recent high-profile homicide in Toronto, the police canvassed certain neighborhoods and requested swabs from the inside of cheeks of hundreds of residents to conduct DNA analysis.[39] The DNA was then checked

---

33. 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" *CBC Online* (14 November 2002), <http://www.cbc.ca/news/features/canadian_id.html>.

34. See American Civil Liberties Union, National Identification Cards, "Why Does the ACLU Oppose a National I.D. Card System?", <http://archive.aclu.org/library/aaidcard.html>.

35. See Dan Farmer & Charles C. Mann, "Surveillance Nation" *Technology Review* (2003), <http:www.technologyreview.com/articles> (citing a report by J.P. Freeman).

36. *Ibid.* See also 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 and G. Armstrong, *The Unforgiving Eye: CCTV Surveillance in Public Space* (Hull: Centre for Criminology & Criminal Justice, 1997).

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

38. See *e.g.* D.M. Tanovich, "Using the Charter to Stop Racial Profiling: The Development of an Equality-Based Conception of Arbitrary Detention"(2002) 40 Osgoode Hall L. J. 149; Jeff Dominitz, "How Do Laws of Probability Constrain Legislative and Judicial Efforts to Stop Racial Profiling?" (2003) A. L. & Econ. Rev. 412. For a discussion of *Charter* issues and racial profiling, see *R. v. Brown* 2003 C.A. 1251 (QL), <http://www.ontarioreports.on.ca/decisions/2003/april/brownC37818.htm>, [2003] 64 O.R. (3d) 161.

39. See CTV News Staff, "T.O. Police Defend Requesting DNA Samples", <http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1053616704997_144/?hub=TopStories>.

against a databank of DNA samples to determine whether an individual could be a suspect. The Canadian *Anti-Terrorism Act* extended the DNA warrant scheme and data bank to include terrorism offences in the list of "primary designated offences" for which DNA samples can be taken and stored.[40]

1.2. Industry Information Collection Practices

1.2.1. Personal Information Protection and Electronic Documents Act

Many of the legal reforms and technology developments are designed to assist governments in their efforts to access personal information that has been previously collected by the private sector. The relationship between laws that govern private sector and government surveillance has thus taken on increased importance in the post-September 11th environment. With the exception of the province 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*).[41] *PIPEDA* along with the federal *Privacy Act*,[42] which regulates government information collection practices, are overseen by the Privacy Commissioner, an independent officer of Parliament.

Beginning on January 1, 2004, all companies doing business in Canada will have to get the explicit or implicit consent of an individual prior to collecting or distributing personal information.[43] A brief examination of some of the main provisions of *PIPEDA* is necessary to assist in understanding the recent changes to the legal regime that surrounds Canadian private sector information gathering practices. *PIPEDA*, in part, was legislated to protect privacy interests in "an era in which technology increasingly facilitates the circulation and exchange of information."[44]

The new legislation only applies to private sector actors that collect "personal information" in the course of "commercial activity." 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."[45] "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."[46] *PIPEDA* does not

---

40. As a primary designated offence, an order will be issued to obtain DNA samples for investigation purposes. If the crime was a secondary designated offence then such an order can only be made if a court approves the order.

41. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*]. For a 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" (2001) 85 Minn. L. Rev. 1171 at 1200–21.

42. *Privacy Act*, R.S.C. 1985 c. P-21, as amended.

43. See Stephanie Perrin, *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.").

44. *PIPEDA*, *supra* note 41 at s. 3.

45. *Ibid.* at s. 2 (1) "personal information".

46. *Ibid. PIPEDA* also applies to collection of personal information about employees who are employed by any "federal work, undertaking or business."

apply to any organization that uses personal information solely for journalistic, artistic, or literary purposes.[47]

The general approach of *PIPEDA* is that the consent of an individual 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 may be implied, based on the circumstances.[48] A subscriber might reasonably expect that a magazine would have implied consent to solicit subscription renewal.[49] But if the magazine wished to sell a list of its subscribers to a third-party direct marketer, it would be appropriate to seek additional, explicit consent because that purpose would be inconsistent with the original consent.[50]

Explicit consent is always required when the personal information is particularly sensitive, such as with medical and financial records.[51] Implied consent is appropriate when the information is less sensitive. Sensitivity should be based on context.[52] For example, subscription lists to certain special-interest magazines could be considered "sensitive" in nature.[53]

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 their personal information.[54]

In addition to notice and consent provisions, *PIPEDA* strives to encourage fair information practices. *PIPEDA* encourages accountability by mandating data collector responsibility for the personal information of a data subject,[55] including information that has been transferred to an unrelated third party.[56] Further, the organization must designate an individual to be accountable for the collection practices (i.e., a Chief Privacy Officer).[57] The organization must also ensure that the personal information is as "accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."[58] The information must be stored in a secure fashion. For example, electronic records can be protected with encryption and audit trails.[59] In addition, upon written request, con-

---

47. *Ibid.* at s. 4 (2) (c). See also s. 7 (1) (c).
48. *Ibid.* at Sch. I, cl. 4.3.4.
49. *Ibid.* at Sch. I, cl. 4.3.5.
50. *Ibid.*
51. *Ibid.* at Sch. I, cl. 4.3.4 –4.4.7.
52. *Ibid.* at Sch. I, cl. 4.3.4 (noting that the "form of the consent may vary, depending on the circumstances, and the type of information").
53. *Ibid.* at Sch. I, cl. 4.3.4.
54. See EC, Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, [1998] O.J. L. 281/31 at para. 7, <http://.europa.eu.int/comm/interna/_market/privacy/docs/wpdocs/2001/wp39en.pdf>. The Directive permits the collection of information in certain circumstances without consumer consent.
55. The terms "data collector" and "data subject" come from the EU Data Protection Directive. Although they are not found in *PIPEDA*, the underlying concepts remain consistent.
56. *PIPEDA*, *supra* note 41 at Sch. I. cl. 4.1.3., which states that an organization is responsible for personal information that has been transferred to a third party for processing. See also EU Data Protection Directive, *supra* note 54 at para. 36.
57. *PIPEDA*. *ibid.* at Sch. I, cl. 4.1, 4.8.2 (a).
58. *Ibid.* at Sch. I, cl. 4.6.
59. *Ibid.* at Sch. I, cl. 4.7.3.

sumers must be provided access to their personal information stored by the organization in order to amend any incorrect information.[60]

1.2.2. Technology Developments

Information technology developments have enhanced the ability of industry to collect detailed information about customers and employees. Businesses have always tracked their customers' behavior (*e.g.*, credit card purchases) and sold this information to third parties, so it is not so much a question of novelty but one of scale and context. Information technology developments now permit an enormous quantity of detailed transactional information to be gathered and stored, and for relationships to be drawn between formerly discrete identities.[61]

Consider the impact of the internet. Industry currently collects information on web site visits through various data mining techniques (*e.g.*, "cookies") and posts literally tens of billions of banner ads each month targeted at customers.[62] Over 90% of commercial web sites gather some form of data about web site visitors.[63] By June 2000, the largest online marketing company, Doubleclick Inc., had compiled databases on roughly 88 million United States households to assist in these direct marketing campaigns.[64]

In addition to internet technologies, the private sector has begun employing a variety of different mechanisms that have privacy-encroaching implications. These technologies include: (a) cell phones that report the precise geographic location of telephone calls; (b) the use by supermarket chains of "smart cards" that track details surrounding all purchases; (c) computer chips within consumer products that provide information on location and usage for inventory control purposes; (d) the use of radio frequency identification (RFID) tags in automobile tires that give information concerning car speed and location; (e) video or camera surveillance to inhibit crimes (*e.g.*, under a municipal bylaw, every taxi in Toronto must have a camera that takes a photograph of every customer) and (f) a variety of electronic monitoring techniques in the workplace to monitor phone calls and computer usage (*e.g.*, keystroke-logging programs that store information on every computer keystroke made by an employee).

1.3. The Relationship between Privacy Laws and Technology

At some point, all of these different surveillance technologies may become integrated within large private sector and government databases. The ability to monitor, store, exchange, cross-index and retrieve digital information grows each

---

60. *Ibid.* at s. 8 (1), s.9 (3). "Access to the personal information need not be granted if, *inter alia*, the information is protected by solicitor-client privilege; the information would reveal confidential commercial information; or the information was collected for law enforcement purposes. Access will also be denied if it would reveal personal information about a third party and that information is not severable from the record."

61. See Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1970). See also Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (Beijing and Cambridge: O'Reilly, 2000) at 70 (for a historical discussion of the emergence of detailed dossiers or "data shadows").

62. U.S., Federal Trade Commission, *Online Profiling: A Report to Congress, Part 2* (July 2000), <http://www.ftc.gov/os/2000/07/onlineprofiling.htm>.

63. *Ibid.*

64. Tom McNichol, "Double Agents" *Wired* 8.06 (June 2000) 124, <http//www.wired.com/wired/archive/8.06/mustread_pr.html>.

year, permitting state agents to access potentially huge amounts of detailed personal information concerning individuals.

Many of the previously discussed efforts, 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 industry databases and could create powerful tools for a "surveillance society." The merged databases could contain detailed personal information about individuals, including their email records, health problems, credit history and credit card purchases, criminal records or interactions with the police, employment histories, telephone records, television shows watched, vacation destinations, and web site visits.

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 agencies."[65] Under the guise of national interest, a government employee, without the knowledge of the individual in question, could scrutinize these merged databases.

To a certain extent, *PIPEDA* works against the trend toward the sharing of information between state and industry actors. For example, *PIPEDA* limits the collection of personal information in many circumstances, which could place less information at the potential disposal of state agents.[66]

Some might argue that the technologies themselves have a neutral value and governments can simply decide one day to stop using them when the risk of terrorism declines. However, technology is partly deterministic in nature, as advancing technology can shape and change the way we live. It is unclear whether the clock can 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 present greater resistance to change: "[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."[67]

While the anti-terrorism laws have been subjected to explicit evaluation prior to implementation, less attention has been paid to the technology developments that surround these policy changes. Technology, however, can introduce significant social changes while escaping the "pattern of deliberation and review" that governs legal changes.[68] The problem is that such inattention to technology developments leads to an increased risk that unanticipated adverse social outcomes will take place.

---

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

66. *PIPEDA*, *supra* note 41 at Sch. I, cl. 4.5 (indicating that personal information shall not be used or disclosed for purposes other than those for which it is collected and that personal information should be retained only as long as necessary).

67. Thomas P. Hughes, "Technological Momentum" in Merrit Roe Smith & Leo Marx, eds., *Does Technology Drive History? The Dilemma of Technological Determinism* (Cambridge: MIT Press, 2001) at 112.

68. For discussion see Paul B. Thompson, "Justice, Human Rights and Ethics Issues" in *Science and Technology Policy, Encyclopaedia of Life Sciences* (Oxford: UNESCO, 2002).

These outcomes include a heightened risk of repression of political dissent as surveillance technologies are used to target identifiable groups such as Muslim Canadians, despite no evidence of individual wrongdoing. Further, pervasive and unseen scrutiny by state agents could inhibit freedom of expression, as individuals fear that the police *could* monitor their speech and actions. There is extensive literature that scrutinizes the trend toward the use of increasingly powerful technologies of surveillance along with possible social ramifications.[69] This literature suggests in part that technology can serve to amplify the legislative changes surrounding surveillance practices. As a result, the growing use of surveillance technologies could ultimately inhibit important democratic values.

*

2. ASSESSING GOVERNMENT SURVEILLANCE PRACTICES

2.1. Empirical Evaluations

At this point, there appears to be very little empirical information that would permit an appropriate assessment of Canadian surveillance practices since September 11, 2001. 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 preventative arrest and investigative hearing provisions.[70] Further, a Parliamentary review of the anti-terrorism legislation as a whole is scheduled to take place three years after the *Anti-Terrorism Act* takes effect.[71]

The Justice Department has provided to Parliament its first annual report on the use of preventative arrests and investigative hearings for the period between December 24, 2001 and December 23, 2002.[72] The report notes that the police did not use either provision during the period under scrutiny.

Section 195 of the *Criminal Code* requires the Solicitor-General to publish an annual report on authorizations granted for interceptions 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.[73] In 2003, the Solicitor-General published its annual report for the year 2001, which covers roughly the four-month period that followed the terrorist attacks on the

---

69. See *e.g.* Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Pantheon, 1977); David Lyon & E. Zureik, "Privacy and the New Technology" in *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 J.M. Balkin, "What is a 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.

70. *Criminal Code*, *supra* note 4 at s. 83.31.

71. See *Anti-Terrorism Act*, *supra* note 3 at s. 145.

72. See Canada, Department of Justice, *Annual Report concerning Investigative Hearings and Recognizance with Conditions* (Ottawa: Department of Justice, 2002), <http://canada.justice.gc.ca/en/terrorism/annualreport.html>.

    See also *Criminal Code*, *supra* note 4.

73. Tyler Hamilton, "Powers Snoop More, Explain Why Less" *The Toronto Star* (24 March 2003) D1.

United States. In 2001, 121 authorizations were granted to monitor private communications.[74] This is less than the number of authorizations granted in each of the previous four years. For example, 150 authorizations were granted in 2000 and 154 authorizations were granted in 1999.[75]

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

Refugees and landed immigrants are likely the group that is most vulnerable to government surveillance in a time when foreign terrorists are perceived to pose the most real security threat. According to the Canadian Council for Refugees, in the period ranging from November 16, 2002 to January 23, 2003 there were on average 446 people detained for immigration-related offences in Canada.[76] This number is roughly equivalent to the detention numbers for previous years.

The Federal government also collects data surrounding complaints filed with the Privacy Commissioner. Between April 1, 2002, and March 31, 2003, the Privacy Commissioner received a total of 1,642 complaints under the *Privacy Act*, which regulates federal government information collection practices.[77] This number represents an increase of roughly 400 complaints from the previous year. Moreover, 300 complaints were received for *PIPEDA* from January 1, 2002 to December 31, 2002, up by 200 complaints from the first year that the statute took partial effect.[78] Finally, in 2002, the Office of the Information Commissioner did not receive any "secrecy certificates" created under the *Anti-Terrorism Act*. These certificates prevent the Information Commissioner from disclosing information concerning government activities.[79]

The empirical evidence of police surveillance practices is clearly limited in the sense that these reports do not offer detailed appraisals of the surveillance practices. The reports also do not assess whether there has been an increase in the use of privacy-encroaching technologies by state agents. Further, the periods under review do not include potential recent developments, due to the time lag involved in compiling data. It may therefore take more time to evaluate government conduct properly.

---

74. Canada, Solicitor General of Canada, *Annual Report on the Use of Electronic Surveillance 2001* (Ottawa: Minister of Public Works and Government Services Canada, 2003), <http://www.psepc-sppcc.gc.ca/Publications/Policing/Electronic_Surveillance_2001_e.asp>.
75. *Ibid.* at 5.
76. Canadian Council for Refugees, "Detention Statistics" (March 2003), <http://www.web.net/~ccr/detention-statscurrent.html> [Detention Statistics].
77. See Privacy Commissioner of Canada, *Annual Report to Parliament* (Ottawa: Privacy Commissioner of Canada, 2002-2003) at 19.
78. *Ibid.* at 56.
79. Information Commissioner of Canada, *Annual Report* (Ottawa: Information Commissioner of Canada, 2002–2003) at 25.

2.2. Anecdotal Reports

There is, however anecdotal evidence that expanded investigatory powers have led some Canadian police and intelligence agencies to label certain groups as "terrorists" to justify the use of these powers.[80] According to media reports, targeted groups have included Native Canadian activists, environmental and anti-globalization protesters, and anti-war activists.[81]

Further, the expanded powers raise the risk of racial profiling in a time of heightened stereotype against minority groups such as Muslims. The Canadian Islamic Congress reports that hate crimes against Canadian Muslims have increased by more than 1,600% since September 2001, and indicates "numerous cases" of warrantless interviews and interrogations of individuals of Muslim or Arab origin.[82]

In addition, there have been media reports of increased use by the Canadian government of "security certificates" under the *Immigration and Refugee Protection Act* in the aftermath of September 11th.[83] The security certificates permit individuals 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 CSIS.[84]

According to a government spokesperson, the government has issued only twenty-seven of these certificates since 1991 and courts have quashed only three of them.[85] Moreover, a Canadian intelligence official has indicated that only five certificates were issued between September 11, 2001 and September 24, 2003.[86] The Canadian Council for Refugees (CCR) has noted that the number of individuals detained for security reasons has declined "more or less steadily" from a period ranging from November 2002 to January 2003.[87] Of post-September 11th security cases, "the statistics show one person on a security certificate in Quebec (since 10 January) and a handful identified as security related, but not on a certificate, and apparently mostly not staying long in detention, in Quebec, Ontario and the Prairies/Territories."[88] The CCR has also noted that recent changes to immigration laws heighten the risk that refugees will be denied permanent resident status because they have fewer legal protections to counter allegations that they pose a security threat.[89]

---

80. For discussion see *In the Shadow of the Law*, *supra* note 18 at 2.
81. *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 Ronald Daniels *et al.*, *The Security of Freedom* (Toronto: University of Toronto Press, 2001) at 168.
82. *Ibid.*
83. For a media report on protests directed at the policies of Immigration Canada, see Andre Picard, "WTO Protest Opens on Quiet Note" *The Globe and Mail* (28 July 2003) A5.
84. Canada, Citizenship and Immigration Canada, *Fact Sheet No. 6, Keeping Canada Safe: The Immigration and Refugee Protection Act*, <http://collection.nlc-bnc.ca/100/200/301/cic/immigration_refugee_act_fact_sheet-e/no06/ci51-111_2002-6-e.pdf>.
85. Sue Bailey, "Detainees' Relatives Demand Ottawa Act" *The Toronto Star* (26 August 2003).
86. See "Security Certificate Use is Rare, MPs Told," *The Globe and Mail* (25 September 2003) (discussing the testimony of the head of the Canadian Security Intelligence Service).
87. See Detention Statistics, *supra* note 76.
88. *Ibid.*
89. See Canadian Council for Refugees, "Refugees and Security" *CCRWeb.net* (February 2003), <http://www.web.net/~ccr/security.PDF>.

The possibility of abusive state surveillance practices has been highlighted by 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.[90] The expert in question had spent the previous fourteen years preparing wiretap affidavits for use by the Ontario Provincial Police. The disclosure has led so far to the dismissal of charges against accused individuals or release of several convicted individuals on the basis that evidence was obtained through illegal wiretaps.[91]

The most egregious Canadian example of post-September 11 state abuses involves a Syrian-born Canadian citizen named Maher Arar. On September 26, 2002, Mr. Arar was traveling home to Canada from a family vacation when he was apprehended by U.S. authorities during a routine stopover in New York to change planes. The U.S. authorities then deported Mr. Arar to Syria due to alleged links to terrorist organizations. In Syria, Mr. Arar was interrogated, tortured and imprisoned for over a year until he was eventually returned to Canada on October 6, 2003. No charges were ever laid against Mr. Arar in Syria, Canada or the United States.

At this writing, it remains unclear why Mr. Arar was deported to Syria in the first place. The Canadian government has admitted that the United States deportation decision was motivated in part by information concerning Mr. Arar that had been provided by Canadian officials.[92] The U.S. officials who questioned Mr. Arar in New York had in their possession a copy of a private rental agreement signed by Mr. Arar in Ottawa in 1997, but Canadian officials have been unable to explain how the private document ended up in U.S. hands.[93] At a minimum, the Canadian government should hold a public inquiry to determine what role that Canadian authorities played in this matter. The inquiry should also scrutinize the sharing of intelligence information between Canadian and American officials to ensure they do not make similar errors in the future.

2.3. Lack of Accountability

Canada and the United States are using or propose to use powerful technologies to amass detailed information about their residents and citizens for security purposes. A danger exists that state agents or other individuals will misuse this information and harm privacy rights and target certain individuals for illegitimate reasons. While the empirical and anecdotal evidence to date does not suggest the emergence of a police state, better accountability mechanisms should be implemented to reduce the risk of abusive surveillance practices.

As surveillance technologies become more prevalent, technology has at least the potential to encourage government accountability. Under cyberlaw theory, it has been pointed out that "code is law": code—the hardware and software

---

90. Christie Blatchford, "Fall of OPP's Wiretap Expert Could Set off Judicial Storm" *The Globe and Mail* (5 September 2003) A1.

91. *Ibid.*

92. "Canada supplied information used against Arar, says solicitor general" *CBC News* (19 November 2003), <http://www.cbc.ca/stories/2003/11/19/arar_ashcroft031119>.

93. Jim Bronskill "CSIS denies role in Arar detention" *CBC News* (23 November 2003), <http://cnews.canoe.ca/CNEWS/Canada/2003/11/23/266407-cp.html>.

technologies that comprise the internet—imposes constraints on the behaviour of internet participants.[94] On this view, regulators ought to pass laws to govern the code in order to achieve a policy goal. The 'Lawful Access' proposal by the Department of Justice represents an attempt to do just that, by mandating that ISPs use certain technologies to ensure that police can track online information.

Similarly, the Canadian government should consider passing legislation that would govern how state agents may use technologies to collect and store personal information.[95] For example, certain forms of particularly sensitive information might be stored in files that required independent judicial authorization to be accessed.[96] For large databases, emerging technologies may permit personally identifying information to be "scrubbed" from search results that are delivered to government analysts.[97] The analysts could then scan these search results to detect patterns of behavior that give rise to security concerns, while any subsequent investigation could focus on individuals whose identities would be revealed after the authorities overcome traditional legal safeguards such as the need to obtain a search warrant. These software solutions would hence permit the collection and aggregation of large quantities of data for sound public policy reasons (for example, to track the Severe Acute Respiratory Syndrome "SARS" epidemic) without maintaining permanent records that disclose individual identity.

The law can also mandate the tracking of information on database searches performed by government agents. By maintaining logs of searches 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.[98] The record will also permit authorities and citizens to correct errors created through surveillance. Further, the fact that searchers will be aware that their computer usage is being recorded will act as a disincentive for abusive surveillance practices.

This approach has been adopted to a certain extent with respect to a recent federal government initiative. As noted earlier, CCRA proposed to create an air traveler database that would retain information concerning these travelers for a six-year period.[99] As a result of sustained criticism by public interest groups and the former federal Privacy Commissioner, the plan was modified in March

---

94. See generally Lawrence Lessig, *Code and other laws of cyberspace* (New York: Basic Book, 1999) at 6.

95. For discussion of the need to employ built-in operational safeguards to reduce potential abuse, see U.S., Defense Advanced Research Projects Agency, *Report to Congress regarding the Terrorism Information Awareness Program 2003* (Washington, 2003) at 33–35, <http://www.darpa.mil/body/tia/tia_report_page.htm>. 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) pre-deployment legal review of the use of surveillance technologies; and (d) spot auditing of surveillance technologies.

96. For discussion, see Dan Farmer & Charles C. Mann, "Surveillance Nation–Part Two" *Technology Review* (May 2003), <http://www.technologyreview.com/articles/farmer0503.asp> (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).

97. For discussion, see Leslie Walker, "Balancing Data Needs and Privacy" *Washington Post* (8 May 2003) E1.

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

99. Canada, Canada Customs and Revenue Agency, *Fact Sheet: Advance Passenger Information/Passenger Name Record* (October 2001), <www.ccra-adrc.gc.ca/newsroom/factsheets/2001/oct/advance-e.html>.

2003.[100] Proposed changes include: permitting access to the information by customs officials for the first seventy-two hours, then restricting access after this date; restricting access to a limited number of intelligence officials; purging information not required for CCRA purposes such as what travelers ordered to eat; and providing that police must obtain a warrant to access information unless exigent circumstances exist.

In addition to technology solutions, the Canadian government ought to have a more focused review of the use by police of emerging technologies to assist with surveillance and investigations. The legal and technological changes in the post-September 11th environment are complex and ongoing. The government should create an independent committee to provide oversight of these changes to ensure that abusive state practices are not taking place. It has also 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 or by ensuring that the Standing Committee on Justice and Human Rights participate in this oversight.[101]

An 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.[102] In 2002, the Canadian government mandated through its Privacy Impact Assessment Policy that every federal program and service undergo a Privacy Impact Assessment (PIA).[103] According to the Privacy Commissioner, Canada is the first country in the world to mandate PIAs for all federal departments and agencies.[104] The PIA involves the preparation of a report to ensure that privacy is protected when an existing or new policy is implemented.[105] A PIA will provide these government agencies with a consistent framework to evaluate departmental policies and procedures to determine their impact on privacy and take mitigating action to overcome problem areas. Between April 2002 and March 2003, the Privacy Commissioner received 17 PIAs and 12 preliminary PIAs.[106] These encouraging efforts could be broadened into an independent examination of the impact of the anti-terrorism legislation on privacy rights and interests.

Finally, more transparency should be encouraged with respect to any state or private sector surveillance measures. For example, laws can mandate the listing of all public areas that are watched by video cameras. The public could access these lists in libraries or perhaps the internet. The lists could include other

---

100. "Big Brother Travel Database Restricted" CBC News (9 April 2003), <www.cbc.ca/stories/2003/04/09/privacy_030409>; Privacy Commissioner of Canada, News Release, "Breakthrough for Privacy Rights" (9 April 2003), <www.priv.gc.ca/media/nr-c/2003/02_05_b_030408_e.asp> (setting out the changes to the CCRA's proposed database).

101. See *In the Shadow of the Law*, *supra* note 18 at 2.

102. In a welcome development, the Office of the Privacy Commissioner has begun to review the impact of anti-terrorism measures on privacy through a review of information gathering practices of the Royal Canadian Mounted Police, the Canadian Security Intelligence Service and the Communications Security Establishment. See Privacy Commissioner Annual Report, *supra* note 77 at 45.

103. Canada, Treasury Board of Canada Secretariat, *Privacy Impact Assessment Policy, 2002*, <www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp>.

104. *Supra* note 77 at 47.

105. *Supra* note 77 at "Policy Requirements."

106. *Supra* note 77 at 48.

helpful information, such as the storage period for information that does not record any criminal behavior. Moreover, these public areas should include signs that warn of surveillance measures.

*

CONCLUSION

I WOULD GIVE THE CANADIAN GOVERNMENT a C+ for its surveillance practices and use of privacy-encroaching surveillance technologies in the two years since the terrorism attacks of September 11th. The government's own data, while somewhat limited, suggest that there has not been a marked increase in the use of electronic surveillance after September 11, 2001. Further, the fact that the controversial preventative arrest and investigative hearing provisions of the *Anti-Terrorism Act* have not been used as of December 31, 2002 suggests that police practices may not have significantly changed. *PIPEDA*, which governs private sector information collection practices, should also serve to inhibit the sharing of personal information between government and industry. Yet, anecdotal reports suggest that possible racial or religious discrimination may be focusing state attention on certain identifiable groups such as Muslim Canadians, despite the absence of evidence concerning individual wrong-doing. It may, however, be too soon to properly evaluate state practices due to the complex and ongoing legal and technological changes that followed the terrorism bombings.

To earn a better grade, the government should take steps to increase public accountability over surveillance practices. This can be accomplished by creating an independent oversight committee that scrutinizes police practices in the post-September 11 environment and by mandating the use of technologies that discourage unauthorized snooping of large government databases.