

**Who Watches the Watchers? Examining the
Relationship between Government and Private Sector Surveillance**

By Arthur J. Cockfield[?]

Introduction

There has been a heightened call for government surveillance in light of the terrorist attacks on the United States. It seems likely that we will become increasingly watched by government agents who can resort to a host of monitoring technologies in an effort to promote greater security, including more surveillance of Internet communications and more surveillance of public spaces by digital video cameras. This paper argues that, in times of crisis under heightened government surveillance, weak legal control over private sector information gathering practices leads to an unacceptable intrusion into privacy rights.

A comparative analysis of the legal regimes in Canada and the United States is offered to shed light upon the relationship between the laws that regulate government information gathering practices and the laws that regulate business practices.¹ Prior to the terror attacks of September 11, both countries had strong legal restraints on government surveillance while the United States, in contrast to recent reform initiatives

[?] 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 and Don Stuart for comments on this earlier draft.

¹ For an early discussion of the relationship between these laws, see ALAN WESTIN, *PRIVACY AND FREEDOM* (1967) (arguing that government surveillance, using increasingly sophisticated tools, is the main threat to privacy rights). More recent concerns surrounding government/business surveillance have focused on issues such as privatization, deregulation and joint ventures. See, e.g., DAVID LYON, *SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE* 143-145 (2001).

in Canada², has relatively weak regulatory control over businesses that monitor private information.

A weak private sector privacy regime leads to the danger of a government-industry partnership where advances in information technologies can be used to amass detailed personal information on individuals, leading to the potential targeting of visible minorities and political dissenters. Perhaps the most fundamental question for any political system, including democracies, is: “Who watches the watchers?”³ Weak or non-existent private sector consumer privacy laws make it more difficult to hold government accountable for its surveillance practices.

The paper is organized as follows. Part I overviews the right to privacy in the context of government and industry surveillance under American and Canadian law. Part II discusses how legal controls over government surveillance have been weakened after the terrorist attacks. Part III describes how a weakened legal regime surrounding government surveillance coupled with weak laws surrounding consumer privacy creates the risk of a government/industry collusion that is watching us, often without our knowledge. Laws that require a consumer’s explicit consent before information can be gathered help to ensure a proportionate surveillance response and the protection of fundamental rights such as the right to freedom of expression.

² Under the new law, Canadian consumers will need to grant their consent to the collection of personal information otherwise industry is not permitted to collect this information. See The Personal Information Protection and Electronic Documents Act, S.C., 2000. Ch. 5 (effective Jan. 1, 2001 for certain federally regulated industries and covering all businesses operating in Canada as of Jan. 1, 2004).

³ The question is derived from ancient latin saying: *Quis custodiet ipsos custodes?* See Decimus Junius Juvenal, The Satires, Book V1, Line 347. Circa A.D. 50-130.

I. Laws That Govern the Watchers

This Part briefly reviews legal constraints against government and commercial efforts to scrutinize personal behavior under American and Canadian law.

A. Government: Reasonable Expectations and Private Spaces

Under early English common law, a legal doctrine emerged that protected an individual's home from unwarranted scrutiny by the sovereign. Hence the saying "A man's home is his castle" and, if one were fortunate enough to own a castle, the king was restricted from barging through the front gates. Over time, a view arose that activities that one conducts in one's own home were generally none of the business of government. Accordingly, the law tends to offer greater protection over private matters that occur in private places like homes (and, to a lesser extent, vehicles).⁴

While there is no general constitutional right to privacy in either Canada or the United States,⁵ the highest courts in both countries have reflected on the important role that privacy plays in our civil democratic societies. The U.S. Supreme Court has argued: "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

⁴ More specifically, the protection against unreasonable searches extends to the person and not the place: an individual's expectations of privacy are influenced by control and ownership he exerts over a particular place. "In my view, the single most important idea that emerges from the jurisprudence is that expectations of privacy must necessarily vary with the context. 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." See *Schreiber v. Canada (Attorney General)* (1998), 124 C.C.C. (3d) 129 (S.C.C.).

⁵ In the United States, the Bill of Rights 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 like abortion or contraception. However, there is no general right to privacy. See, e.g., *Bowers v. Hardwick* [cite]. For detailed discussion on the Canadian approach, see DON STUART, *CHARTER JUSTICE IN CANADIAN CRIMINAL LAW* (3rd.ed., 2001).

Amendment.”⁶ The Canadian Supreme Court has similarly noted the critical role of privacy: “Society 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 from prying into the lives of the citizen go to the essence of a democratic state.”⁷ The Canadian 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.’”⁸

Both Courts articulated their views on privacy in the context of constitutional protections offered against government searches. For instance, section eight of the Canadian Charter of Rights and Freedoms reads: “Everyone has the right to be secure against unreasonable search or seizure.” The Fourth Amendment to the U.S. Constitution contains a similar prohibition against unreasonable searches.⁹ These constitutional protections generally prevent government agents from using technologies to scrutinize private activities unless the police go before an independent judge to secure a search warrant issued on the basis that there is probable cause that criminal activity is taking place. Courts have interpreted these constitutional protections to take into account technological developments. For example, the U.S. Supreme Court has recently held that the use by police of thermal imaging technologies that scan for heat (in order to locate

⁶ See *Olmstead v. U.S.*, 277 U.S. 438 (1928) (Brandeis dissent). Brandeis’ dissent eventually became the majority view in later Supreme Court decisions.

⁷ See *R. v. Dyment* (1988), 2 S.C.R. 417, 427 (S.C.C.).

⁸ See *R. v. Mills*, 28 C.R. 207, 251 (1999) (S.C.C.).

⁹ The Fourth Amendment indicates: “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.”

high-intensity lamps needed for marijuana growing) constitutes an impermissible search.¹⁰

The general thrust of legal decisions in both the United States and Canadian courts is to protect “reasonable expectations” of privacy.¹¹ A reasonable person, for example, may expect to be left alone in her home but has reduced expectations when she leaves her home. Accordingly, a court might not have any constitutional concerns surrounding government-initiated video surveillance in a downtown urban center because an individual would not be seen to have a reasonable expectation that she would not be watched in this public place.

Beyond these constitutional protections, Canada and the United States have federal laws that prevent government agencies from collecting or trading in personal information in many circumstances. In Canada, the federal *Privacy Act* limits the federal government’s ability to collect personal information in some circumstances and permits Canadians to access and correct personal information about them that is being held by government organizations. The United States appears to have fewer federal protections surrounding the collection and distribution of private information by federal government agencies. The *Privacy Act of 1974* contains provisions which mandate fair information practices, but permits disclosure of personal information for routine uses that are associated with a federal agency’s goals. Further, the *Electronic Communications Privacy Act of 1986* protects the right to private communications in many instances and,

¹⁰ See *Kyllo v. U.S.*, _ U.S. _, 121 S. Ct. 2038 (2001);

¹¹ See, e.g., *Hunter v. Southam Inc.*, (1984), 41 C.R. (3d) 97 (S.C.C.). For recent U.S.-Canada comparative analysis, see Robert W. Hubbard, Peter DeFreitas & Susan Magotiau, *The Internet—Expectations of Privacy in a New Context*, 45 CLQ 170 (2001). See also David E. Steinberg, *The Drive Toward Warrantless Auto Searches: Suggestions from a Back Seat Driver*, 80 B.U. L. REV. 545 (2000).

although initially intended to establish constraints on the use of wiretaps, is becoming increasingly applied to the Internet and other digital media.¹²

Canada has a federal privacy czar—the Privacy Commissioner—whose mandate includes monitoring violations of privacy laws and ensuring that information gatherers are held accountable for their actions. There is no U.S. equivalent to Canada’s Privacy Commissioner although the U.S. federal Office of Management and Budget participates in setting privacy policies for federal agencies. Both countries additionally have provincial or state legislation that restricts the collection and distribution of personal information in certain circumstances (e.g., that prevent government agencies from selling personal information derived through driver licenses).¹³

In summary, Canada and the United States generally had strong legal protections against government surveillance prior to the terrorist attacks.

B. Commerce: Ubiquitous Information Collection Practices

Information technology developments have enhanced the ability of industry to collect detailed information on its customers or 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 newness, but more a question of scale. Information technology developments now permit an enormous quantity of detailed information to be gathered and stored concerning individual identity.

Consider the impact of the Internet. Industry currently collects information of web site visits through various data mining techniques (e.g., “cookies) and posts literally

¹² See, e.g., *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035 (9th Cir. 2001).

¹³ See, e.g., *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, Chap. F.31.

tens of billions of banner ads each month targeted at customers.¹⁴ Over 90% of commercial web sites gather data on web site visitors. By June 2000, the largest online marketing company, Doubleclick Inc., had compiled databases on roughly 88 million U.S. households to assist in these direct marketing campaigns.¹⁵ But industry, unlike government, has an ostensibly benevolent purpose behind these information collection practices: they are simply trying to sell products to consumers who can choose to reject the goods or services.

The United States and Canada have taken different paths in the context information collection practices by commercial actors. The U.S. generally follows the industry self-regulation model where companies are expected to self-regulate their information gathering techniques. Self-regulation has been promoted under efficiency and equity rationales.¹⁶ In theory, a company will align its information gathering techniques with the privacy needs of its customers: it's 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.¹⁷

Consider the ongoing debate surrounding the use of “cookies” planted in the hard drive of consumers in order to data mine web site visitors: cookies are used to track web

¹⁴ For discussion, see Federal Trade Commission, *Online Profiling: A Report to Congress* (June 2000), available at www.ftc.gov.

¹⁵ See Tom McNichol, *Double Agents*, *Wired*, June 2000, at 124.

¹⁶ Self-regulation is thought to be more efficient because policy makers feared that countless new online privacy laws from governments around the world would inhibit the development of e-commerce. Privacy laws would effectively “gunk up” the network inhibiting information flows, especially in the more financially important business-to-business market on the Internet. Self-regulation also protects equity interests because commercial free speech is not restricted under this approach. For discussion, see PETER P. SWIRE & ROBERT E. LITAN, *NONE OF YOUR BUSINESS, WORLD DATA FLOWS, ELECTRONIC COMMERCE AND THE EUROPEAN PRIVACY INITIATIVE* (1998).

¹⁷ 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 *Minnesota Law Review* 1171, 1200-1221 (2001).

site visits in part to permit marketing profiles to be amassed on web surfers. Cookies also perform useful functions by remembering passwords, permitting web pages to be personalized and so. Consumers have the ability to reject all cookies (or control cookies through more advanced settings) by modifying options available on their web browsers. This probably does not prevent a challenge for sophisticated users, but polls suggest that a typical Internet user would have great difficulty in changing his browser settings to reject cookies.

Under the self-regulation model, industry should presumably respond to this problem by creating an easier way to control or stop the privacy-inhibiting effects of cookies. For example, why not place a graphic of a chocolate chip cookie at the top of the browser so that Internet users could accept or reject cookies by clicking on the graphic? Or perhaps consumers could “click” on a part of the cookie to engage more advanced options such as permitting benevolent cookies (e.g., cookies that remember passwords). This would seem like a fairly straight-forward market response to the poll-supported view that individuals are concerned about their online privacy rights.

But the browser market does not resemble anything like an environment of perfect competition that would encourage an appropriate industry response under the self-regulation model. There are effectively only two browsers in the market: Microsoft Internet Explorer and Netscape’s Navigator. Both Microsoft and AOL/Time-Warner (which owns Netscape) have vested interests in maintaining the *status quo* surrounding data mining techniques. Neither company presumably wants to make it easier to have their own cookies rejected along with a loss of revenues from third party advertisers that pay for banner ads. In any event, the fact that there are only two companies that provide

the vast majority of consumers from the U.S. and Canada with access to the World Wide Web suggests very little need to innovate privacy-enhancing technologies; an unspoken collusion may occur in an environment with so little competition.¹⁸

Outside of the browser market, industry has responded by creating trusted third party online intermediaries that place a seal of approval on web sites that follow privacy guidelines.¹⁹ Further, a number of companies provide “identity management” technologies to Internet users to mask or anonymize their identities. The most popular company is San Diego-based Anonymizer.com that uses a proxy server to mask the identity of its customers. The technology permits the company to reveal the identity of its customers upon being presented with a search warrant or subpoena. In contrast, Montreal-based Zero Knowledge Systems, uses a complicated network of servers to anonymize consumers; this technology prevents even Zero Knowledge from discovering the identities of its customers, hence frustrating any potential police investigation. In the current environment, political pressure may be employed to reduce the use of such technologies because they permit terrorists (and other criminals) to communicate without fear of detection.²⁰ Any potential restrictions on these anonymizing technologies may, however, be counter to principles of freedom of expression that are given broad constitutional protection in Canada and the United States.

Despite the emphasis on self-regulation in the United States, there exists a trend toward greater administrative oversight by the Federal Trade Commission and, prior to

¹⁸ Entrants into the browser market-place may be inhibited by network effects; the fact that so many users currently employ one of the two products which may come bundled with operating systems (in the case of Microsoft) or Internet access software (in the case of AOL/Time-Warner).

¹⁹ See, e.g., www.truste.org.

²⁰ Soon after this after, Zero Knowledge Systems Inc. announced that it would stop selling its Freedom consumer privacy product (in order to concentrate on enterprise network security solutions) although the company plans on introducing another consumer privacy product.

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, namely notice, choice, access and security. In addition, federal U.S. legislation sometimes uses a sectoral approach to protect certain forms of personal information such as financial records, medical records, or information concerning children.

Personal Information Protection and Electronic Documents Act

Canada generally pursued a self-regulatory approach until the passage of the *Personal Information Protection and Electronic Documents Act* that will cover all business information collection practices as of January 1, 2004.²¹ The Internet was largely responsible for this legislation: Canadian regulators feared that privacy concerns were inhibiting the development of e-commerce and they wanted to bring their own privacy policies into concordance with recent European Union initiatives as well as the Organization for Economic Cooperation and Development (OECD) norm.²² The Canadian legislation compels companies to obtain an individual's explicit consent before these companies collect, use or disclose personal information.

While many companies follow an "opt out" approach under the self-regulation model (i.e., consumers are entitled to notify the company that they do not want their activities to be monitored), the Canadian approach—similar to the European Union's so-

²¹ The Act took effect on January 1, 2001 for certain federally regulated businesses such as banks, telephone companies and interprovincial transportation. On January 1, 2002, the Act applied to all organizations that collect, use or disclose health information. The Act applies to all businesses operating in Canada beginning January 1, 2004. See note 2.

²² The Canadian legislation was based on the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information, which in turn was based on OECD fair information gathering practices. The current OECD norm is based on information gathering practices that began in the early 1980s. See OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1981). The OECD norm was followed within Europe soon after. See Council of Europe, Convention for the Protection of Individuals with Regards to the Automatic Processing of Data (1981).

called Privacy Directive as well as the OECD approach—encourages an “opt in” approach. All companies (including U.S. companies) doing business in Canada will have to get the consent of an individual prior to collecting or distributing personal information.²³ The main difference between the U.S. and Canadian approach is that consent to information gathering is an implicit element of the contract between consumers and businesses in the U.S. whereas this consent must be explicitly given by consumers in the Canadian context. Further, the Canadian federal Privacy Commissioner—an independent ombudsman—is provided with the authority to ensure companies are held accountable for their information gathering practices.

a. Purpose of the Act

The Act, in part, strives to:

Establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.²⁴

b. Scope of the Act

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

²³ Note, however, that there is an exception for the collection of information needed by a law enforcement agency for an investigation.

²⁴ ¶ 3.

including the “name, title or business address or telephone number of an employee of an organization.”²⁵ “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.”²⁶ The Act does not apply to any organization that uses personal information solely for journalistic, artistic, or literary purposes.²⁷

c. General Approach: The Need for Consumer Consent

The general approach of the Act is that the consent of an individual must be obtained before personal information can be collected, used, or disclosed. The expectations of a “reasonable person” determine whether consent must be express, or may be inferred, based on the circumstances.”²⁸ An example is provided where a person who subscribes to a magazine could reasonably expect that the business would contact the subscriber in the future to solicit a renewal of the subscription.²⁹ Accordingly, the act of subscribing serves as a means of consent for the later contact. But an individual would not reasonably expect that personal information given to a health care professional would be given to a company that sells health care products, unless consent was obtained.³⁰

Further, the use of personal information is limited to purposes for which it was collected otherwise additional consent must be obtained from the individual. Consent, however, is not required “where inappropriate.” It is suggested that

²⁵ ¶ 2(1).

²⁶ ¶ 2(1). The Act also applies to information collection of personal information about employees who are employed by “federal work, undertaking or business.” ¶ 2(1).

²⁷

²⁸ ¶

²⁹ ¶ Schedule 1, ¶ 4.3.5.

³⁰ Id.

express consent is required when the personal information is considered sensitive such as occurs with respect to the collection of medical and income records.³¹ Implied consent is appropriate when the information is less sensitive. Sensitivity should be based on context. For example, subscription lists to certain special-interest magazines could be considered “sensitive” in nature.³²

d. Fair Information Collection Practices

In addition to notice and consent provisions, the Act strives to encourage fair information practices suggested by the CSA and the OECD. The Act encourages accountability by mandating that the information gatherer is responsible for personal information in its possession, including information that has been transferred to a unrelated third party. Further, the organization must designate an individual to be accountable for the collection practices (e.g., a Chief Privacy Officer). Further, the organization must 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.”³³ The information must be stored in a secure fashion. For example, electronic records can be protected through encryption and passwords.³⁴ In addition, consumers, upon written request, shall be provided access to personal information stored by the organization in order to amend any incorrect information.³⁵

³¹ Sched. 1, ¶ 4.3.6.

³² Sched. 1, ¶ 4.3.4. Knowledge and consent are additionally not required in the following circumstances. Collection is permitted when ... Use is permitted without knowledge and consent when the information ... Disclosure is permitted without knowledge and consent when the information is...

³³ Sched. 1, ¶ 4.6.

³⁴ Sched. 1, ¶ 4.7.3.

³⁵ Access to the personal information need not be granted if, inter alia, the information is protected by attorney-client privilege, the information would reveal confidential commercial information or the information was collected for law enforcement purposes.

With respect to remedies, the federal Privacy Commissioner is empowered to receive complaints, to conduct investigations, and to attempt to resolve complaints.³⁶ The Commissioner can also initiate complaints in certain circumstances. If the matter cannot be resolved by the Commissioner then a Federal Court can hear the dispute.³⁷ Court remedies include: (i) ordering an organization to correct its practices; (ii) ordering an organization to publish a notice of any action taken or proposed for correcting its practices and (3) awarding damages to the complainant, including damages for humiliation suffered.

The new Canadian laws can be justified from an efficiency perspective because the legislation is now harmonized with world-wide norms of forcing companies to get explicit consent before they gather personal information. The U.S. approach, on the other hand, is counter to world-wide trends and hence a concern arises that data flows may be inhibited as companies struggle to implement two divergent privacy policies.³⁸ The Canadian approach can be additionally supported on equity grounds despite the fact that the new laws will inhibit commercial free speech to a greater extent than the self-regulation approach: the enhanced protection of individual privacy—especially in light of heightened government surveillance—trumps these commercial free speech concerns.

In summary, Canada has implemented stronger legal protections for consumer privacy in comparison to the general self-regulation approach in the United States.

³⁶

³⁷

³⁸ The U.S. requests companies to voluntarily enter into “safe harbor” arrangements with the European Union in order to comply with the EU Directive.

II. The New World: Weakened Legal Control over Government Watchers

In the wake of the terrorist attacks, the Canadian and American governments have both introduced legislation that would expand the surveillance powers of government employees to monitor or intercept communications. At the time of this writing, it is unclear which legislative efforts will prove successful although a few developments can be noted.

A. Reduced Expectations of Privacy

As discussed, constitutional protections against government searches are based largely on reasonable expectations of privacy. Courts may grant greater constitutional latitude to government surveillance measures in light of the terrorist attacks because individuals have reduced privacy expectations in times of conflict: privacy is sacrificed to promote greater security.³⁹ Further, the Canadian federal government could argue that broader surveillance powers are justifiable under Section 1 of the Charter as a reasonable infringement on rights in a free and democratic society arising from domestic security concerns.

B. Reduced Judicial Scrutiny

Legislation in both countries contemplates reduced scrutiny by judges over government surveillance efforts. For example, 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 other measures

³⁹ 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 (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 of Rights and Freedoms, but were still subject to common law (and legislative) prohibitions against unreasonable search and seizure.

are aimed at enhancing the ability of government to conduct digital surveillance of its own residents and residents in foreign countries.⁴⁰ For example, the *Combating Terrorism Act* (passed by the Senate on September 13) includes provisions that would increase the government's ability to monitor and seize email messages and web site visits (without resort to a court for a traditional search warrant).⁴¹ Under a lower threshold test where 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 email destinations and the information contained in the to/from header, how long the message was, whether any attachments were included as well as a list of all web sites visited.⁴²

Compulsory national identification cards have surfaced as a possible legislative priority. Polls taken in the U.S. and Canada suggest the majority of the public supports such initiatives. These cards already exist in many countries and are used to access public services such as health care or to prevent welfare fraud. These cards can be embedded with detailed information concerning an individual, including the possible use of biometrics (e.g., a digitized thumbprint embedded in the card). The Canadian government has announced that it will fast-track legislation promoting high technology ID cards for new immigrants. The ACLU and other organizations have traditionally

⁴⁰ Other proposals include: using information collected by foreign governments against U.S. citizens even if the information was obtained illegally under U.S. constitutional standards; compelling ISPs to provide credit card information on alleged terrorists through a subpoena (and not under the normal higher-threshold court order); placing wiretaps in national security investigations.

⁴¹ In theory, the U.S. government already has the ability to access certain information concerning emails and web sites without resort to a search warrant. The U.S. Supreme Court has held that information such as a list of telephone number dialed by an individual is does not create a reasonable expectation of privacy and as such does not raise Fourth Amendment concerns. Under the federal government's interpretation of current law, the government can already access this information just like it can do with telephone number lists with so-called pen registers and trap and trace devices.

⁴² More specifically, the section 832 of the Combating Terrorism Act of 2001 permits, under the lower threshold, the collection of information such as telephone numbers dialed as well as "routing, addressing, or signaling information."

opposed the use of national identification cards because they can foster discrimination and harassment against certain identifiable minority groups and could be used as a tool to repress political dissent.⁴³

Finally, 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 against a database of suspects. This type of surveillance is already fairly prevalent in parts of the world like England—the average British citizen is photographed or caught on video an astonishing eight to three hundred times every day⁴⁴—although critics question the efficacy of the approach.

Facial recognition technologies pose an additional danger surrounding racial profiling; if the terrorists are of suspected Middle Eastern origin then this increases the chances of someone from this identifiable group will be mistaken by digital video surveillance as a potential suspect. In other words, people from an identifiable group will be watched more closely than others despite an absence of evidence concerning any individual wrong-doing. Computer surveillance technologies are not infallible: 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 the Canada and the United States under constitutional protections surrounding the right to be free from discrimination on the basis of race, ethnicity or religion.

C. No Government Oversight

Government accountability is abolished for all intensive purposes when laws do not require any independent actor like a judge to review government searches. Under

⁴³ See www.aclu.org/library/aaidcard.html.

⁴⁴ See Vito Pilieci, March Unveils Surveillance System, *Ottawa Citizen*, Sept. 28, 2001, at E1.

proposed legislation, Canada and the United States plan to grant broader powers to their intelligence services to monitor private communications. Public accountability over searches conducted by intelligence services is often refused on the grounds that public awareness of these searches could jeopardize investigation or place sources at risk. In part, spies have been kept in check in the past due to a lack of resources: spies just did not have sufficient technical, capital or human resources to scrutinize residents of their own countries. In the wake of September 11, the Canadian and American governments have announced significant increases in the budgets for intelligence organizations, enabling these organizations to expand their surveillance techniques.

For example, an increased use in technologies that watch 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 unfortunately named Carnivore), which permits investigators to sift through an ISP's emails. Due to the global nature of the Internet and the fact that Internet traffic originating in the U.S. is often routed by ISPs into Canada before crossing the border again to arrive at a U.S.-based destination, Carnivore is suspected to monitor Canadian web traffic and emails.⁴⁵

Canadian legislators are similarly considering laws to extend the reach of electronic surveillance mechanisms, partly in response to public security concerns and partly as a result of political pressure applied by its southern neighbor.⁴⁶ While a Carnivore-like program is not (openly) used by CSIS or other branches of the

⁴⁵ See Tyler Hamilton, *FBI Software Can Take Bite out of Canadians' Privacy*, *Toronto Star* (March 25, 2001).

⁴⁶ Canadian regulators often pursue a policy of regulatory emulation in contexts such as taxation due to relative importance of the American economy to Canada. See Arthur J. Cockfield, *Tax integration under NAFTA: Resolving the Conflict between Economic and Sovereignty Concerns*, 34 *Stanford Journal of International Law* 39 (1998).

government,⁴⁷ Canada does participate 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.⁴⁸

Proposed Canadian legislation would permit a Minister to issue a certificate, based on the guise of national security, that would prevent Canadians from accessing personal information that has been collected by the Canadian government. The federal Privacy Commissioner has opposed these developments on the grounds that the certificates would permit the government to circumvent existing privacy laws that encourage government accountability over its information gathering practices.⁴⁹

D. Note on Technology and Surveillance

Government surveillance can be conducted with increasingly sophisticated electronic surveillance means. Writing in 1928 on the growing use of telephone wiretaps, Justice Brandeis recognized that technology could lead to increasingly 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.”⁵⁰

⁴⁷ Bill C-36 expands the ability of the Communications Security Establishment to monitor or intercept communications between Canadian citizens and “foreign targets.” There will be no judicial oversight for this monitoring although a Minister must issue a certificate before the surveillance can go forward.

⁴⁸ See Ursula Sautter, *Electronic Surveillance: How the State Can Spy on You*, Time.com (July 28, 2000).

⁴⁹ See George Radwanski, *Testimony regarding Bill C-36, the Anti-Terrorism Act*, to the House of Commons Standing Committee on Justice and Human Rights (Oct. 23, 2001) located at http://www.privcom.gc.ca/speech/02_05_a_011024_e.asp

⁵⁰ *Oslmstead v. U.S.*, 277 U.S. 438 (1928).

Technological developments such as satellite, cell phone or email surveillance have made it easier for government to watch us without being noticed.⁵¹ The ability to monitor, store, exchange, cross-index and retrieve digital information grows each year, permitting state agents to access potentially huge amounts of detailed personal information concerning individuals. A weakened legal regime surrounding government searches will presumably increase the use of emerging surveillance technologies that watch us without our consent or notice.

III. The Road Ahead: Who Watches the Watchers?

This Part discusses how a government/business surveillance partnership (i) can collectively amass detailed personal information on individual identity; (ii) may unduly limit privacy by creating an environment where individuals fear they might be constantly monitored by state agents relying on business information collection practices; and (iii) will make it more difficult to hold government accountable for its information gathering practices.

A. The Potential for a Government/Business Surveillance Partnership

As discussed, business has traditionally had a much freer hand in its pursuit of private data concerning its customers in comparison to the restrictions placed on government. For example, a 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 to be an illegal search if conducted by government.⁵²

⁵¹ For a discussion of emerging surveillance techniques, see Paul Kaihla, *Weapons of the Secret War*, *Business 2.0*, Nov. 2001 at p. 98.

⁵² See *In re Doubleclick Inc. Privacy Litigation*, ___ F. Supp. 2d (S.D.N.Y. 2001).

Government has traditionally been prohibited from accessing data compiled by a business unless government agents follow stipulated legal procedures such as getting a search warrant. But, once the legal process has gone its course, government will be able to access the records compiled by industry. The check in the system has always been the high legal threshold imposed on government search efforts. To the extent that this threshold is lowered in times of crisis, weak legal prohibitions against business information gathering efforts indirectly benefits government surveillance needs. Business in effect does the grunt work of information gathering and storing for the potential day when government needs to access this information.

In order to understand the implications of a government/business surveillance partnership, consider the following hypothetical example. TVcorp is a television cable station based in Rochester, New York that provides cable services to consumers located throughout the North-Eastern states in the United States as well as parts of Ontario and Quebec. TVcorp implements a monitoring technology that tracks the viewing habits of the subscribers to its digital cable services. The monitoring technology makes a record of every television program that is viewed, including the amount of time spent watching each program. TVcorp sells a list of the recorded viewing habits to third party marketing companies who want to gauge audience demand for certain television shows.

The FBI obtains a warrant to attach a special computer consol to TVcorp's main servers. The software program within the computer consol scans the database of viewing records to locate individuals who have watched certain shows such as a series of Biography specials on known terrorists. These viewers are cross-indexed against other

viewing records that indicate the subscribers watched TV programs concerning certain fundamentalist religious practices.

Armed with this knowledge, the FBI begins, through its sniffer program installed at TVcorp, monitoring the viewing habits of specific individuals who are never told that their viewing habits are being watched and may be unaware that such detailed surveillance is possible in the first place. Or perhaps member of the public learn that government/industry *could* be tracking their viewing habits. On the margin, this may inhibit viewing “controversial” programming (i.e., programming that does not conform to the norm with respect to socio-political beliefs, human sexuality, etc.).

Linking government databases with industry databases would create powerful tools for a surveillance society. The merged databases could contain detailed personal information about individuals, including their voting record, 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 argues, “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.”⁵³ Under the guise of national interest, these merged databases could be scrutinized by a government employee without the knowledge of the individual in question. A weak legal regime surrounding consumer privacy encourages this process.

B. Lack of Proportionality

⁵³ David Lyon, *Facing the Future: Seeking Ethics for Everyday Surveillance*, in *Ethics and Information Technology* (forthcoming 2001)

Industry has a vested interest in promoting the development and implementation of digital surveillance technologies.⁵⁴ Industry wants access to customer information for efficiency reasons (e.g., legitimate marketing purposes). Government wants access to personal information for efficiency reasons as well (e.g., reduction of administration costs), but also for broader public policy purposes such as national security. But the need to promote security must be balanced against other public interest concerns surrounding the need to protect privacy rights.

In light of the terrorist attacks, an argument can be made that we should encourage businesses to share personal information with the state in order to promote greater security. At the time of this writing, it remains unclear whether the terrorists used information technologies to plan or carry out their attack. Some news reports suggest the terrorists used encrypted email, satellite phones and an elaborate information technology infrastructure to plan and carry out the attacks. Other reports indicate that the alleged attackers feared monitoring devices (through past experience) and preferred word-of-mouth or other forms of oral or written communication that could elude surveillance technologies. The attack itself was decidedly low tech, involving knives, box cutters and presumably threats or actual uses of brute force against passengers or employees in the planes.

Hence it may be too early to tell whether increased business/government surveillance would help to either catch the attackers or prevent similar attacks in the

⁵⁴ In a widely reported item, the CEO of Oracle, Larry Ellison, indicated his support for a national ID card embedded with digital fingerprints. Ellison said that Oracle would donate software to help to create the cards. Conspiracy theorists: note that Ellison's first customer was the CIA.

future.⁵⁵ In our modern technology-swamped world, there may be an almost knee-jerk response to look to technical solutions to problems that may have nothing to do with technology. The Internet has clearly assisted investigators in forming a web of contacts to gather evidence and search for clues, but it remains unclear whether the Internet or other digital media will prove effective at protecting national security.

The danger is that a business/government partnership will lead to individuals being increasingly watched by unseen forces of government and industry. As our lives become increasingly tied to digital media (PDAs, digital television, computers and the Internet, cell phones, etc.), our actions and thoughts may become increasingly subjected to scrutiny by one of the partners. Digital records are perfect records, down to potentially the most minute detail—every web site we visit, every email we send, every keystroke we make—creating a potentially permanent record of our activities and thoughts.

The nature of digital information and its accompanying distribution system facilitates the collection, exchange, manipulation and storage of information. A government/industry surveillance partnership could abolish the right to be left alone, a foundational right that secures the right to freely express oneself. We have always been watched to a certain extent, but digital surveillance exponentially increases the ability of others to gather and store information about us.

The knowledge of this potential scrutiny may change our behavior in significant ways.⁵⁶ It makes us take greater care before we visit a web site or tap out a few thoughts

⁵⁵ See Don Stuart, *On the Need to Recodify Criminal Law and Rise Above Law and Order Expediency: Lessons from the Manitoba Warriors Prosecution*, *Manitoba Law Journal* (forthcoming 2001).

⁵⁶ A body of literature generally produced by sociologists examines the impact of surveillance technologies on our societies. See, e.g., David Lyon & Elia Zureik, *Surveillance, Privacy, and the New Technology*, in

on our word processors. If an individual thinks that their activities (web site visits, television viewing, impromptu “Singing in the Rain” dance in a downtown center, etc.) will somehow be stored and potentially used against her in the future, she may change her behavior and in so doing edit her expression. But free citizens should be granted great latitude to express careless thoughts and words, to possess careless viewing habits and fantasies, to express themselves in ways that harm nobody.

C. Lack of Accountability

The ancient saying “Who watches the watchers?” queried what political institutions are necessary to ensure that a government is held accountable for its actions. A government/business surveillance partnership makes it more difficult to hold accountable state agents for their actions. Without strict government oversight, industry can amass personal information on individual identity often without consent or knowledge. Government can sit by the side to allow this information gathering process to go forward then, under weakened legal restraints, collect all of the detailed information it requires.

Business/government surveillance that exclusively tracks terrorists is of course not the problem. The main problem is that secret surveillance will be turned against political dissent or other classes of vulnerable individuals such as refugees—all under the guise of national security. According to a report commissioned by the European Parliament’s Civil Liberties Committee, surveillance technologies are justified under state interest rationales but are often used to monitor political dissent, journalists,

Computers, Surveillance & Privacy 1 (1996); James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (1986).

minorities and political opponents.⁵⁷ The report concludes that surveillance technologies exert a powerful chill effect on individuals who may wish to take a dissenting viewpoint and deters others from exercising their democratic right to protest government policy.

To the extent that industry/government surveillance is shrouded in secrecy, people may become less trustful of their government and may fear retribution if they express anti-government opinions: industry or the government *may* have stored somewhere information that can be used against the potential dissenter.

Further, the institutionalization of industry/government surveillance practices may result in a citizenry that is increasingly complacent about this scrutiny. After all, pervasive scrutiny by unseen forces may one day become the norm (many would argue it already is). We may become increasingly undemocratic to the extent that we cease to review potentially abusive state actions. Perhaps we will increasingly fail to ask: who is watching us? Who is monitoring, tracking, compiling, editing, sorting and distributing information about us?

Quis custodiet ipso custodes? Who watches the watchers?

Conclusion

As a result of the terrorist attacks, legal protections surrounding government surveillance will be reduced as individuals become more willing to sacrifice privacy in order to benefit from enhanced security. This paper has argued that weak legal protections surrounding business information gathering practices permit government actors to significantly expand their surveillance powers. Overly intrusive monitoring by an industry/government surveillance partnership may ultimately inhibit critical values

⁵⁷ See European Commission's Science and Technology Options Assessment Office, *Assessing the Technologies of Political Control* (1997).

such as the right to be left alone and the right to freedom of expression. The argument supports the view that states should protect privacy rights by passing laws that force businesses to get explicit consent from their customers before these businesses are permitted to gather, store or distribute personal information.