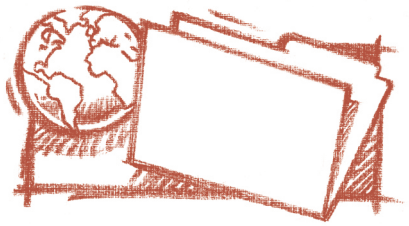
THE FRASER INSTITUTE

STUDIES IN DEFENCE & FOREIGN POLICY



Number 3 / October 2004

Privacy and Security
in an Age of Terrorism

Barry Cooper

Calgary Policy Research Centre, The Fraser Institute

Contents

A FRASER INSTITUTE OCCASIONAL PAPER

Studies in Defence and Foreign Policy are published periodically throughout the year by The Fraser Institute.

The Fraser Institute is an independent Canadian economic and social research and educational organization. It has as its objective the redirection of public attention to the role of competitive markets in providing for the well-being of Canadians. Where markets work, the Institute's interest lies in trying to discover prospects for improvement. Where markets do not work, its interest lies in finding the reasons. Where competitive markets have been replaced by government control, the interest of the Institute lies in documenting objectively the nature of the improvement or deterioration resulting from government intervention. The work of the Institute is assisted by an Editorial Advisory Board of internationally renowned economists. The Fraser Institute is a national, federally chartered non-profit organization financed by the sale of its publications and the tax-deductible contributions of its members, foundations, and other supporters; it receives no government funding.

To order additional copies of Studies in Defence and Foreign Policy, any of our other publications, or a catalogue of the Institute's publications, please contact the publications coordinator via our toll-free order line: 1.800.665.3558, ext. 580; via telephone: 604.688.0221, ext. 580; via fax: 604.688.8539; via e-mail: sales@fraserinstitute.ca.

For media enquiries, please contact Suzanne Walters, Director of Communications via telephone: 604.714.4582; via e-mail: suzannew@fraserinstitute.ca.

To learn more about the Institute, please visit our web site at www.fraserinstitute.ca.

The author of this study has worked independently and opinions expressed by him are, therefore, his own, and do not necessarily reflect the opinions of the members or trustees of The Fraser Institute.

Editing, design and typesetting: Kristin McCahon and Lindsey Thomas Martin

Printed and bound in Canada

ISSN 1702–0263 Studies in Defence and Foreign Policy (Print)
ISSN 1702–0271 Studies in Defence and Foreign Policy (Online)

Date of issue: October 2004

The Fraser Institute, Fourth Floor, 1770 Burrard Street, Vancouver, BC, V6J 3G7

For information about membership, please contact the Development Department:

in **Vancouver**

- via telephone: 604.688.0221 ext. 586; via fax: 604.688.8539
- via e-mail: membership@fraserinstitute.ca

in **Calgary**

- via telephone: 403.216.7175 or, toll-free 1.866.716.7175;
- via fax: 403.234.9010; via e-mail: barrym@fraserinstitute.ca.

in **Toronto**

- via telephone: 416.363.6575;
- via fax: 416.934.1639.

Executive Summary

In the summer of 2004, the Attorney General of British Columbia responded to the BC Information and Privacy Commissioner who had expressed his official concern that the extraterritorial application of the USA Patriot Act posed a threat to the privacy of British Columbians and other Canadians. Given the extensive and effective mechanisms in place for cross-border sharing of information on suspected and convicted criminals, the use of the USA Patriot Act by American officials is both unnecessary and unlikely.

Security and privacy are not, in fact, part of a zero-sum game. Rather they are complementary social realities. An analysis of the notion of security in terms of the distinction between identity and behaviour indicates clearly that surveillance of behaviour enhances security without threatening privacy.

There are some legitimate concerns that the widespread application of biometric technologies threatens privacy; several additional concerns have been raised over Bill C-36, the Canadian antiterrorism bill, which seem to be exaggerated and alarmist. Such criticism as exists regarding Canadian antiterrorism efforts ought more properly be directed against the lax and inadequate application of existing laws rather than against the laws themselves.

Canada & the USA Patriot Act

On July 23, 2004, the Government of British Columbia made public its submission to the BC Information and Privacy Commissioner, David Loukidelis, who was conducting an analysis of the implications of the USA Patriot Act (United States, H.R., 2001) for the privacy of British Columbians (Province of British Columbia, 2004). The Privacy Commissioner has an official interest in the implications of the American law because the Government of British Columbia routinely out-sources government services to US-based and US-linked providers of database services in much the same way that Canadian companies routinely maintain and manage American data. This is one of the many trade benefits made possible by Article 105 of NAFTA, Article I:3 of the General Agreement on Trade in Services, which is part of the WTO agreement, and by similar international trade and investment agreements.

The Privacy Commissioner was concerned, first, whether, and under what circumstances, the USA Patriot Act would give American authorities such as the FBI or the department of Homeland Security access to personal information about British Columbians that is held in American data banks. Second, if the USA Patriot Act did authorize American access to Canadian information, he was concerned about the extent to which the American law conflicts with the Freedom of Information and Protection of Privacy Act (FOIPP Act), a British Columbian statute governing access to, and control of, personal information provided by the government to all service providers whether resident in British Columbia or not.

The release of the submission by Attorney General Geoff Plant was front-page news in the *Vancouver Sun* (Kines, 2004) and, on the same day, was the subject of a column by Vaughn Palmer (Palmer, 2004). Both the reporter and the columnist emphasized the provision of the USA Patriot Act that authorizes the FBI (for example) to obtain confidential information from private sources such as data management companies and at the same time to do so under conditions that prohibit the company from disclosing to the targetted individual (or to anyone else) that the authorities had an official interest in the information obtained. That is, American law-enforcement agencies can order information to be produced by third parties such as an employer and ensure that the target never knows of their interest. Both Kines and Palmer claimed that this was a threat to the privacy and civil liberties of both Canadians and Americans.

The USA Patriot Act was passed following the terrorist attacks of September 11, 2001. Its official title, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, indicates that it was drafted as part of an intelligence and counter-terrorism package of laws, regulations, and directives. It was passed by overwhelming majorities in both the House (357 to 66) and Senate (98 to 1) and became law in six weeks, a remarkably short time for such a complex and constitutionally ambitious piece of legislation. Clearly, it was part of the general political response to the terrorist attack of September and reflects in law many of the patriotic emotions of the day. As with so many other aspects of the war against terrorists or, to be more precise, against al-Qaeda, the boundary between the criminal justice system and the military is ambiguous. We consider the implications of this issue for Canadians below (page 15).

Now, it is an axiom of intelligence gathering that you do not want to let targets know you are interested in them. A modest amount of reflection suggests that the secrecy with which information is obtained about targets under the provisions of the USA Patriot Act or any other security legislation is simply common-sensical, at least in terms of intelligence gathering. After all, a target who is a terrorist is likely to ensure operational security prior to the actual attack by acting clandestinely

in planning and preparing the action. Accordingly, the last thing any intelligence agency would want to do is let this individual know he was under surveillance or that the agency was suspicious that he might be hiding his true and hostile intentions. At the same time, there is no doubt that authority to observe an individual secretly—to "surveille" in intelligence jargon—does pose a threat to that person's privacy and so to his or her civil liberties. Gaining access to private information without advance judicial notice, as occurs with a conventional search warrant, or without subsequent judicial review, means that the "reasonableness" of a search need never be determined or decided by a court. No knowledge of a search means no opportunity to contest its "reasonableness," a constitutional term of art in both the Canadian and American constitutions.

There is, in other words, a *prima facie* conflict between security concerns embodied (at least in principle) in the USA Patriot Act and privacy concerns, in this case raised specifically by the BC Privacy Commissioner and by Attorney General Plant. This paper will (1) analyze the issues involved in this apparent conflict, (2) propose a better way of understanding the tension between privacy and security than as trade-off or zero-sum game, and (3) discuss the Canadian antiterrorism legislation both in the context of the tension between privacy and security and of the wider efforts to deal with terrorist threats, especially al-Qaeda. We begin, however, by surveying the existing arrangements for sharing information between government agencies in Canada and the United States, the immediate and concrete context within which the BC Information and Privacy Commissioner raised his concerns.

Agreements before 9/11

The chief means by which American police and other law enforcement agencies obtain information from Canadian sources regarding security threats is by invoking the Mutual Legal Assistance Treaty (MLAT), which was signed in 1985 and came into force in Canada in 1990 (US Senate, 1988). Under the provisions of the MLAT, American authorities can have access to information held in Canada or held by Canadian governments to the same extent that Canadian authorities can. The initial step in obtaining information from the foreign source (reciprocally for both the United States and Canada) is for the requesting authority to seek the assistance of the government where the information is located.

First resort under MLAT

This "first resort" provision provides the basis for a great deal of routine cross-border cooperation during the investigation phase, which may precede arrest and indictment or the laying of charges, as well as during the subsequent phase of prosecution and trial. Most of this activity deals with ordinary criminal offences and most of that falls under the heading of commercial crime. This includes such practices as illicit telemarketing from one country into the other, deceptive marketing, fraud, antitrust violations, and so on. Moreover, most of the requests under the MLAT deal with documentary evidence and are handled by the executive branch of government in the two countries—crown prosecutors in Canada, district attorneys in the United States, and occasionally higher ranking officials such as attorneys general. These initial requests are not usually subject to judicial review or notice. Likewise it is a domestic executive decision whether or not to grant the request for assistance from the other side. In short, the MLAT has in recent years been the preferred means of obtaining and sharing information (Snow, 2002). Whatever the conceptual differences between terrorism and criminality, an issue to which we return below, investigations of terrorism as well as of other information-gathering operations, are likely to be initially advanced as criminal investigations under the MLAT for the obvious reason that terrorists conduct criminal behaviour by striking at civilians and noncombatants, notwithstanding their typical self-understanding that they are warriors of one sort or another.

The actual procedures involved are also administratively clear. For instance (and hypothetically), the FBI's Field Office in Seattle might make a request under the MLAT for evidence or other information that might be obtained by a search warrant executed in Vancouver. The request would go to the office of the BC Attorney General, in this instance, for approval; the request for a warrant would then be heard by a judge who may then issue the appropriate order. According to circumstances, the search warrant may be executed in cooperation with the American authorities or by Canadians acting alone. Once the information is obtained, in this example by the execution of a Canadian search warrant, but prior to remitting the potentially evidentiary information to the United States, another Canadian judge, who, in turn may impose conditions on what may be sent, must issue an approval order.

Grand-jury subpoenas

Should executive officials in the two countries be unable to reach an initial agreement about sharing information—in the example just given, should the Attorney General of BC refuse an MLAT request originating from the FBI's Field Office in Seattle—the Americans might request a grand jury to issue a subpoena. Under American law, the jurisdictional reach of a subpoena extends to the boundary of the court district in which the grand jury sits. Thus Canadian companies, and their data, are subject to grand-jury subpoenas only to the extent that

they are also subject to the jurisdiction of the relevant court. This means that information held by Canadian companies doing business in the United States would be subject to the jurisdiction of American courts and might be compelled to turn over information about their Canadian or other non-American operations.

At the same time, however, the adverse political consequences of using the authority of grand-jury subpoenas in 1984 to compel the Bank of Nova Scotia to produce information regarding Scotiabank branches in the Bahamas and Cayman Islands has led the US Department of Justice to become increasingly reluctant to seek the extraterritorial application of American procedures and laws. Indeed, they now require police and prosecutors to obtain permission from the departmental Office of International Affairs (OIA) before they can apply for a grand-jury subpoena issued to persons or entities residing in the United States for records located elsewhere. Generally speaking the OIA has been unwilling to approve what are now often referred to as "Bank of Nova Scotia subpoenas."

In short, because the MLAT procedure is the usual way for American authorities to obtain evidence from Canada, neither the USA Patriot Act nor the extraterritorial use of grand-jury subpoenas is likely in the future to provide the legal authority for American officials to seek Canadian evidence—for the same reason that the Scotiabank episode proved embarrassing to American officials. And the decision to agree or not to an MLAT request from the other side resides entirely with the national authorities where the evidence or other information is sought.

Other agreements

There are in addition administrative agreements between the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) and their American counterparts that govern the sharing of information among security agencies in the two countries under the provisions of the Bilateral Consultative Group on Counterterrorism, established in 1988. The Canada-US Cross-Border Crime Forum and the Canada-US Extradition Treaty, in the words of Justice Minister Anne McLelland, also "facilitate [Canada's] ability to work together [with the US] to fight terrorism" (*Hansard*, 2001). Generally speaking, routine information sharing and other forms of coordination and cooperation are undertaken if they meet the "consistent use" test, which means that both Canadian and American authorities share legitimate investigative interests and that, in Canada, it is legal for Canadian authorities to obtain the information. These executive agreements operate outside the MLAT framework.

The USA Patriot Act

As noted above, the USA Patriot Act was an initial legislative response to the attacks of September 11, 2001. Technically, it consisted of a number of amendments to the Foreign Intelligence Surveillance Act (FISA) originally passed in 1978. Section 215 of the USA Patriot Act in particular expands the discretion of law-enforcement authorities beyond that provided even by grand-jury subpoenas. By the same token, the reluctance of the United States to extend subpoena jurisdiction extraterritorially is likely to be at least as important in the application of the USA Patriot Act. Indeed, it is almost inconceivable that the Americans would apply the provisions of the USA Patriot Act to Canada without the active assistance of Canadian governments. That is why the MLAT procedures were established; that is what the RCMP and CSIS counterterrorism agreements with American counterparts are meant to cover.

We agree, therefore, with the conclusion of Attorney General Plant in his submission to the BC Privacy Commissioner, that the USA Patriot Act and, we would add, any likely additional amendments to the statutory authority governing American foreign-intelligence gathering are likely to pose "only a small incremental risk" to the privacy of Canadians. The use of s.215 of the USA Patriot Act to obtain information is not just a last resort, it is also a resort reserved for the worst case. This sanguine conclusion about the USA Patriot Act and Canada does not, however, obviate the need for a more focussed analysis of the relationship between security and privacy, which is conditioned by the notion of risk, even a "small incremental risk." It is to that issue we now turn.

The Tension between Privacy & Security

Privacy looks like a simple thing: it concerns the sensation we experience when we have the power to control information about ourselves and when we actualize that power in conformity with our interests, aspirations, and desires. Inevitably, therefore, there is a personal or subjective dimension to privacy. Some people, for example, do not wish anyone to know for whom they have voted; others place candidates' signs on their lawns or knock on their neighbours' doors to urge them to vote for the candidate whom they support. Such people have a sense of privacy that does not imply that they keep their voting preferences to themselves.

Privacy & security as a zero-sum game

In terms of actual behaviour, privacy implies that other people and, especially, governments or the state are unable to know what we do unless we give them permission. Privacy is connected to liberty not only by liberal theory and the doctrine of natural rights but in the common-sense observation that, if the state knows what we do, the state may directly interfere in our doing of it, whether or not we consent to that interference. In the example noted above, it is up to me whether I advertise my voting preference or not. In a state where privacy is secure, no one can compel me to place a sign advertising a candidate or a party on my lawn. We will see that matters are more complex than is described in this first formulation but it is a good place to begin because the issue of privacy (and more broadly of civil liberties) is typically construed as a zero-sum game (Austin, 2001) in which the entailed trade-off exists between citizens' demands for privacy and citizens' demands that the state protect them from attack, even if state action requires a sacrifice of individual rights for the greater public good. Benjamin Franklin once famously expressed the problem, and left no doubt where he thought the trade-off should be made, in his observation that "they that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." In an era of electronic, real-time, and passive surveillance but also of nuclear war, dirty bombs, and sneak attacks by terrorists, it is worthwhile examining just what constitutes essential rather than trivial or unessential liberty, and what amounts to a little temporary safety rather than a great deal of long-term safety. Indeed, these contemporary novelties lead us to reconsider the validity of the notion that privacy and security are best understood in terms of Franklin's trade-off.

Privacy & security in Canada

There are several reasons why at present in Canada it is at least as important to raise questions concerning privacy and security as it is to provide answers. First of all, most of the discussion to date on this question has been undertaken by lawyers concerned chiefly with technical legal matters more than with broad public policy. Second, most of this discussion, which has by and large been critical of Canadian antiterrorist legislation, "proceeds from the American optic, or the perception of the Canadian initiatives as being no different from the American" (Cotler, 2002/03). One reason that critics have adopted the "American optic" is that by so doing they are able to criticize the Canadian legal response to terrorism along with American policy on counterterrorism and the implications, which were nearly always seen to be malign, it has for Canada. In the present analysis, we will also consider issues and examples from American experience, though we do not adopt an "American optic." The fact is, not only have American analysts grappled with the implications of the alleged trade-off between security and privacy longer than others, Canadian authorities have, at least for the near term, formally integrated many of their security procedures with those of the United States. Accordingly, Canadians ought, as Attorney General Plant said, begin

some serious consideration of issues of great importance to both countries individually as well as to the two countries taken together (Province of BC, 2004).

Privacy & security in the United States

In the United States, some trade-offs between privacy and security have, apparently, already been settled. The Total Information Awareness (TIA) project was initiated in 2002 by the Pentagon under the direction of retired Admiral John Poindexter (the former National Security Advisor in the Reagan administration who was indicted for his part in the Iran-Contra scandal). The objective of the TIA project was clearly indicated by its title and, not surprisingly, was widely seen as a grave threat to privacy and civil liberty (Crewes, 2002a, 2003; Peña, 2002). An alarmed response by civil libertarians as well as by ordinary politicians soon led to the project being cancelled and to the resignation of the program director. Like the USA Patriot Act, TIA was unquestionably an emotion-driven response to 9/11 but one that was widely held to have tipped the balance too far in the direction of security over privacy and liberty. At the same time, to borrow a slogan from World War II, "loose lips sink ships:" notwithstanding the risk to individual liberty, privacy, and freedom of speech, the state has a legitimate security interest in what citizens may say and do, and with whom. In order to simplify the issue and render it more manageable, we assume the existence of a tacit connection between privacy, individual liberty, rights, and freedoms, all of which are meant to be secured by both the Canadian Charter of Rights and Freedoms and by the Constitution of the United States. If we are clear about the relationship of privacy and security we can see what difference, if any, is made by the existence of a political environment characterized by terrorist threats.

Behaviour & identity

We begin, following Demchak and Fernstermacher (2004a; 2004b), by distinguishing two constituent elements of privacy, behaviour and identity. Keeping one's behaviour private means preventing others from knowing *what one does*; keeping identity private means preventing others from knowing *who one is*. Complete privacy, which includes both elements, amounts to invisibility. If security agencies neither know who terrorists are nor what they are doing, they have a major problem. If one must choose between behaviour and identity, it is more important to know what a hostile individual is doing than to know who he is, not least of all because "identity theft" is easy. That is, intelligence focused upon behaviour provides more compelling evidence of an intention to harm than does intelligence concerning identity. Moreover, as Demchak and Fernstermacher emphasized, a focus on identity "not only will inevitably damage civil liberties—perhaps irreparably in terms of lives disrupted—but it will also result in political responses that will fail to provide adequate security, while simultaneously threatening privacy, by creating institutions that inefficiently use new technological tools" (2004b: 4). An important implication of the distinction between behaviour and identity is that the relationship between security and privacy is not necessarily that of a trade-off or zero-sum game. Security procedures directed at the detection of threatening behaviour and then at its prevention can have the result of ensuring not only safety but of safeguarding identity.

Consider video surveillance, for example, a common method of enabling security personnel to monitor behaviour in convenience stores, banks, airports, elevators, parking garages, university campuses, highways, and any number of other public places. Video cameras can provide real-time information on what people are doing within camera range but do not provide information on who is doing it. Security personnel at Wal-Mart or Holt Renfrew are understandably more concerned with what people do in their stores than with who comes in. Usually security personnel in retail stores sit in front of a bank of television monitors. They are alert to observe, for example, individuals stuffing goods into purses or backpacks, under their skirts or down their pants. Typically, however, they do nothing to establish the identity of the target until he or she exits the store without paying for the purloined item. First the behaviour of an individual, namely shoplifting, arouses the initial interest of security personnel; only then does the issue of the shoplifter's identity arise. Moreover, surveillance of shoppers benefits shoppers by contributing to lower shoplifting rates, the costs of which would otherwise be passed on to consumers in the form of higher prices. The identity of non-shoplifters is never an issue, though their interests are served by surveillance.

Surveillance techniques that begin by watching for suspicious behaviour can also be directed at the deadly threat posed by terrorists to the nation. "Surveillance of the means that terrorists employ," that is, their behaviour, Carter wrote,

> is potentially more important than surveillance of persons [that is, their identity], and raises far fewer civil liberties issues. Placing all Middle Eastern male noncitizens resident in the United States under surveillance, for example, is both objectionable and impractical. But inquiring after all those persons, of whatever nationality, who take flying lessons but are not interested in learning to take off or land, who rent crop dusters, or who seek information on the antibiotic resistance of anthrax strains or the layout of a nuclear power plant is feasible and might be extremely useful. (Carter, 2002 19)

Likewise it makes more sense to protect important but vulnerable public buildings such as the Houses of Parliament or the US Capitol with sensitive radiation or anthrax detectors than to restrict access or try to register every vehicle or individual who comes into the vicinity of these sites (Carter, 2002).

Identity & the technology of surveillance

Recent innovations in the technology of surveillance have gone some distance to bridge the gap between behaviour and identity. For example, biometric monitoring systems, which include digitized fingerprints, voiceprints, iris and retina scans, "computerized knowledge assessment" or brain-prints, and hand geometry can, in principle, provide security personnel with a unique identifier—an identity (Kirsch, 2001; see also CCLE, n.d., and associated URLs). Possibly the least intrusive biometric monitoring is to add a computerized face recognition package to a standard video camera (Zhao et al., 2003). The purpose of a face-recognition system is to match images taken from video cameras, which is to say, all individuals who come within camera range, whatever their behaviour, with the images of known individuals. Such systems have, in fact, been tested and are in use.

Even before the terrorist attacks of September 11, 2001, security officials were concerned that a large spectator event would present an attractive target for terrorists. In February 1991, Super Bowl XXXV was held in Tampa, Florida; local and state police were concerned that it might be a magnet for criminal activity or perhaps even a terrorist attack. Accordingly, they sought help from a security provider, in this instance a firm called Viisage, to video surreptitiously the 100,000 fans entering Raymond James Stadium. Using a software system called FACEfinder, images of the fans were captured and compared with a rogues' gallery of images of known criminals and otherwise hostile individuals (see Bowyer, 2004). The images were analyzed with a complex algorithm that measured the angles between geometric points on the face such as nostrils, eye corners, and so on to produce a "faceprint" akin to a digitized fingerprint. The "Snooper Bowl" experiment, as critics called it, made a possible identification of 19 petty criminals—pickpockets and the like—who were in the stands (Chachere, 2001). No arrests were made, no records were kept, and no databases were created. It was an experiment and it proved the technology worked.

Not everyone was pleased. According to Ed Markey, a Democratic Congressman from Massachusetts, "the notion that 100,000 people were subject to video surveillance and had their identities checked by the government" was "chilling" (quoted in Grossman, 2001: 57). In fact what took place was quite different. When police really check your identity, they may look at your driver's licence or fingerprint you. Face recognition technology identifies only those individuals whose biometric identities are already in the electronic gallery or "watch-list," to use a more conventional term. In the Super Bowl experiment 99,981 attendees had no match with anyone on the watch-list and 19 people were possible matches. In no sense did FACEfinder check 100,000 identities. The serious question regarding privacy and security in this example concerns the criteria used to put someone's image in the biometric gallery prior to surveillance. In Tampa, they were crooks whose mugs were well known to the local police.

Criteria unlikely to offend most civil libertarians have been developed to include some people on watch-lists or to include their biometric data in an electronic gallery. For example, if an arrest warrant had been issued, the individual could be included without much concern.

But there are other examples that raise some serious privacy issues. What if someone were merely wanted for questioning? Or what if the police wanted to keep tabs on a suspect's movements? Once on a watch-list, how long would an individual remain there? Would the individual know if he or she were on the list? How? Should a judge be required to issue a warrant similar to those authorizing wiretaps before someone could be placed on a watch-list? Or would something like the assent of a special tribunal, such as was established under FISA to approve surveillance of suspected foreign agents, be sufficient? Once images are digitized, how long can they be archived? Can they be shared with other agencies? These and similar questions do not answer themselves. Moreover, the use of biometric technologies, as is true with all technology, is readily susceptible to "function creep." Just as automatic transponders for toll roads can also be used in court to determine the location of a vehicle in a matter unrelated to the convenience of paying for a toll assessment automatically, if an archive of biometric images exists, the probability that it would be used for unanticipated purposes is high. Like any group of bureaucrats, the police are easily tempted by mission creep, especially when new technologies make it easy.

Consider another example. Cameras take pictures today of vehicles running a red light and the information on the licence plate is used to issue a summons to the registered owner. There is little technical difference between taking a single snapshot and taking a continuous video. If a video camera also has the capability of optical recognition it can scan traffic for a specific vehicle. If such cameras are net-worked, continuous surveillance is possible; database technology makes the surveillance system capable of creating a permanent record of all vehicles surveilled. As with a digitized rogue's gallery there are some uses of traffic surveillance that are unexceptionable. So long as yellow-light intervals at intersections are not reduced, few people would object to red-light-snapshot traffic cameras (Crews, 2002). It is not at all clear, however, that giving the police the capability to catalogue in a permanent database the movements of all vehicles is such a good idea (Harper, 2004).

The Fourth Amendment of the US Constitution, like s.8 of the Canadian Charter of Rights and Freedoms, provides legal guarantees against unreasonable search or seizure. The present concern is with searches rather than seizures. Originally restrictions against unreasonable searches were considered an invasion of one's property rights, a trespass. But since under the common law neither eye nor ear could trespass, initially there was no prohibition on observation or on eavesdropping by the state so long as it did not involve trespass or other violation of property rights. Judicial decisions in both the United States and Canada have changed the right protected by a prohibition against unreasonable searches from property to privacy, or from places to persons.

In this context, Woodward has argued that the use of face recognition technology, which is essentially a passive form of information acquisition, cannot in law be construed as a "search" (Woodward, 2001). With respect to genuine search, the requirement that it be "reasonable" means that there must be probable grounds for suspicion that the person so searched is engaged in wrongdoing. Otherwise the person has a reasonable expectation of privacy. However, Woodward argued, a person does not have such an expectation with regard to public, physical characteristics, including facial features and voice, just as under the common law neither the eye nor the ear could trespass.

On the other hand, critics of this position argue that such an understanding of a reasonable expectation of privacy was formulated prior to the invention of face identifying technologies. Thus, the scale of contemporary surveillance operations means that the traditional understanding of privacy and what is a "reasonable search" must also be changed. Others have said that it is sufficient simply to notify members of the public that they may be entering an area where biometric surveillance is in operation. In some instances there are probably no grounds to object to a faceprint. For example, given the current inconveniences owing to increased security procedures at airports today, getting your picture taken before boarding a plane looks like a relatively minor inconvenience. On the other hand, whereas this may be true enough, the inconvenience of innocent passengers is not the real issue, which is the construction of a biometric terrorist watch-list with which an airport faceprint might be compared. Here matters may be more questionable.

To return to the easier example of Super Bowl XXXV, Woodward concluded that, even if face-scanning were

considered a search, it would be reasonable so long as officials "limited their actions to simply comparing scanned images of people entering the stadium with their computer database of suspected terrorists and known criminals." In this case, there would be no privacy issues involved "so long as no information about individuals were retained, disclosed, or linked to any other database" (Woodward, 2001: 7). Woodward's answer to the question raised earlier as to whether digital images could be archived (and for how long) or shared with other agencies is clearly negative.

Libertarians contemplating only catching pickpockets at the Super Bowl would probably find this an acceptable conclusion. As Eugene Volokh observed, "at least in some situations," and he had Super Bowl XXXV in mind, "camera systems can promote both security and liberty" (Volokh, 2002). Unfortunately, the condition Woodward set for the absence of privacy issues is difficult to enforce because of the aforementioned bureaucratic "mission creep." Moreover, with respect to the issue of preemptive action in the face of terrorist threats, it may also be counterproductive. Historically, it has been acceptable to respond to hostile actions by non-state actors such as drug mobs in an *ex post* fashion using the normal tools of the criminal law. Today, following the catastrophic killing of 9/11, with a massive attack on a densely populated civilian target, foreknowledge of, and preemptive action against, a non-state actor are more prudent activities than punishment and retribution, however necessary the latter course may be.

Actionable intelligence & preemptive action

In order to obtain "actionable intelligence" or useful foreknowledge that can direct preemption, it is necessary to collect information about individuals—and thus seek to obtain identities of persons who have not (yet) commenced hostile behaviour. The implications for the apparent antinomy between privacy and security posed by terrorist threats are thus both novel and serious. "The unfortunate reality of today's world," write Demchak and Fenstermacher, "is that effective preemptive action will require greater invasions of privacy to identify those planning action" (2004b: 8). The reason for preemption is, obviously, that the costs of an *ex post* response are deemed unacceptably high.

This argument also implies that linked databases will be necessary. Historically, in both Canada and the United States, databases dealing with health, finances, education, vehicle ownership, and so on have been legally distinct and often have been legally segregated. This means that multibase "data-mining" by governments is impossible. Under the American counterterrorism laws, it is possible to mine a large database of public and private records (Peña, 2003). Under Canadian law, generally speaking, databases are kept only for specific purposes so that statutes that require information to be reported to the government—tax returns for example—include restrictions on the use to which that information can be put. Because the whole point of antiterrorist laws is to collect information on a wide population of potentially threatening individuals and, equally importantly, their accomplices, and assuming that these massive, merged databases can, in fact, be mined effectively to search for "suspicious" patterns, the attractiveness to security agencies is as obvious as the threat posed to privacy and civil liberties (Crewes, 2002).

Additional privacy issues arise in view of the fact that the collection of data for security purposes may be secret. Indeed, there is not much point in collecting security intelligence if it is to be made public. A comparison of how erroneous information is handled in the private sector illustrates the problem. If inaccurate information is contained, for example, in an individual's financial or credit file, it can be corrected by long-established procedures. Even if it takes a week or two, no serious or irreparable damage is done. On the other hand, if this same inaccurate data is passed on to a secret security file that places an individual, for example, on an airport watchlist, there would be no way that a wrongly detained passenger could challenge a security guard in any reasonable time, certainly not in time to catch a plane.

Because both preemption and linked databases combine identity and behaviour and especially because they emphasize the former, they pose serious problems for privacy. As the example given in the last paragraph indicates, the potential inconveniences for innocent parties are high. The obvious safeguard is to ensure that verification is thorough and an appeal on the basis of false information can be undertaken quickly. Unfortunately, this is much easier said than done. The reason is not simply

because, for example, it would be technically and administratively difficult to enable an airport security guard to challenge the validity of the data that put someone on an airport watch-list that is triggered just before that person seeks to board a plane. The fact is there are problems involved with all identification systems because they can and do make different kinds of mistakes.

Recall the face-scanning experiment at Super Bowl XXXV. Previously, the technology had been used in the private sector to identify individuals whom, for example, a property-owner did not want on the premises: a disgruntled former employee or a gambler with a successful system, a card-counting photographic memory, or fast hands in a casino. For these limited and specific purposes, the technology worked reasonably well; but its purpose was to identify individuals who were well known to the system in the sense that the biometric data was accurate. A card-counter, for example, would have been previously detained by casino personnel because of his winning behaviour; they would have photographed him (perhaps clandestinely but accurately so far as biometrics is concerned) and entered that data into an in-house database. If the card-counter returned, he would be identified prior to recommencing his winning ways. This means that the probability of falsely concluding there was no relationship between the biometric data and the real world of a card-counting casino client—what statisticians call a Type II Error—was low.

The probability of a Type II Error with respect to mass screening is higher, partly because the biometric data that goes into a database of potentially hostile individuals is more likely to be of lower quality owing to poor lighting, bad angles, and so on, especially if the images are acquired surreptitiously. Experimental evidence acquired under favourable conditions confirms these concerns. A year or so after the Super Bowl XXXV experiment, a second one was conducted at Palm Beach International Airport. It resulted in a positive match rate of about 47% and a false-alarm rate of around 0.4% (Bowyer, 2004: 19). That is, the probability of making a Type II error was around 0.5. In terms of its application to specific threats, a 50% correct identification may be high enough to deter hijackers from trying to make it on to planes protected by the system. But, perhaps not. On the other hand, is a 0.4% false-alarm rate, or what statisticians call a Type I error, also acceptable? This amounts to two or three individuals an hour being detained by mistake because of Type I errors. That is, falsely concluding that there is a relationship between the biometric data and the real identity of an individual two or three times an hour may well prove intolerable to airline passengers forced to miss their flights for no intelligible reason other than that provided by probability theory. When the trade-offs between Type I and Type II errors are applied to the much larger numbers of potential terrorists contemplated by the successor to the TIA, called the Terrorist Information Awareness program (and also abbreviated as TIA), the chances of actually nabbing a terrorist has been estimated at .02%. nearly zero (Peña, 2003).

Conclusions

The foregoing analysis of privacy in terms of behaviour, identity, and information allows for a number of conclusions. Granted that no identification system is perfect, and recalling that, generally speaking, private-sector surveillance places greater emphasis on behaviour than identity, in principle, this approach may serve as an initial or default position for government security initiatives as well. Such an approach would certainly meet the many vociferous objections raised in both Canada and the United States against racial profiling, which amounts to a kind of "collective identity" categorization and certainly is largely independent of behaviour (Choudhry, 2001; Choudhry and Roach, 2003). That is, race, education, ethnicity, and religion are poor predictors of an intent to harm. Purchasing a one-way airline ticket for cash is more suspicious than having parents born in Lebanon. Taking level-flight lessons on a 757 simulator but showing no interest in learning to take off or land is more worthy of attention than having visited Iran.

We have seen that modern techniques of database analysis, including data-mining, can generate new information by collating existing information sources. The problem for the privacy of citizens as distinct from that of consumers is that governments have much greater power over individuals than do private information-gathering organizations. It is more important, therefore, for government security agencies than for credit-checking agencies to follow "good cause" procedures. Since

their purpose is to link behaviour and identity, it is even more important for government agencies to minimize the probability of a Type I Error. This means ensuring that validation processes are redundant and appeal processes are rapid. The speed and comprehensiveness of current information technologies that make it possible to track millions of individuals and to monitor their behaviour clearly enhance security. The same technologies are capable of redundant validation of targetted identities and speedy appeal when an individual claims to have been falsely identified. A general, indiscriminate, and Orwellian invasion of privacy can be avoided if security systems are designed to monitor, first, behaviour and, then, identity. A balance between security and privacy is certainly possible, even in the information age threatened with terrorism.

Implications for Canadians

BC Attorney General Plant indicated that the extraterritorial application of the USA Patriot Act posed a "small incremental risk" to the privacy of Canadians. In the previous section, we provided an analysis of the relationship between security and privacy. These same arguments apply to Canadian security legislation, chiefly the Anti-Terrorism Act, or Bill C-36 as it is usually called. The provisions of this law, important in themselves, are even more significant because of the volume of trade between Canada and the United States and the widespread view that, for Americans, "security trumps trade."

Is terrorism an act of war or a crime?

Should terrorism be considered an act of war or a criminal act/ This is particularly important because of what is almost a Canadian consensus on this issue, that terrorism is a crime. Whatever one thinks of this opinion (and the author is of the view that it is erroneous), it is important to be clear about the issue. There are, of course, war crimes but they are acts committed during an unequivocal war that violate agreed-upon rules and conventions regarding the conduct of war. The issue here is whether terrorist acts such as those of 9/11 are acts of war at all.

It is possible to resolve this issue in terms of the theory and practice of international politics and international law or by reference to classical sources such as Clausewitz to determine what war essentially *is* (see Cooper, 2002; 2004: ch. 1). In the present and much more practical context, however, we should look at the actual and contingent response to 9/11 by the American and Canadian governments.

First, some history. Between 1988 and 1998, there were three major terrorist attacks on the United States: the explosion in December 1988 aboard Pan American Flight 103 over Lockerbie, Scotland effected by two Libyan intelligence officials; the bombing of the World Trade Center in February 1993 by Islamists inspired by the "blind sheikh," Omar Abdel Rahman; and the bombing of the American embassies in Nairobi and Dar es Salaam in August 1998 by al-Qaeda. The first two attacks were dealt with entirely within the international or national criminal justice system; the embassy bombings were followed by a unilateral military strike of cruise missiles into Afghanistan and Sudan along with criminal proceedings and convictions against four individuals who were apprehended in New York (Weiser, 2001).

The attack of September 11, 2001, in contrast, was widely denounced as an unprovoked act of war. American authorities launched a criminal investigation that quickly identified al-Qaeda as responsible. The President on October 7, 2001 issued a statement indicating the United States would make no distinction between terrorists and states that harboured them and that the American response would consist of military as well as political, diplomatic, financial, and intelligence efforts. The Congress granted permission to the President to use military force to prevent future terrorist attacks and, by early November 2001, American forces were on the ground in Afghanistan. This deployment certainly looked like a military response, which is to say, a war. As Wesley Wark observed, if we are not formally "at war" we are "at least in a war. Our problem is that we don't understand the nature of this war on terrorism, or its future" (Wark, 2001: 290).

Meanwhile, the domestic response in both the United States and Canada also looked very much like a move to a wartime posture. Hundreds of foreign nationals were detained and questioned; the US Congress passed laws providing the Justice Department with new investigative and surveillance powers, effectively ending the distinction between foreign intelligence operations and domestic law enforcement (Toobin, 2001). In addition the President, as Commander-in-Chief, issued an order to the United States Department of Defence to establish

military tribunals to try Taliban and al-Qaeda fighters, some of whom were captured in Afghanistan by Canadian forces.

In short, prior to 9/11 the preponderant aspect of the American response to terrorism was to apply the relevant criminal provisions of the US Code (18 U.S.C., para. 2332b). Clearly the events of September 11, 2001 were also formally criminal acts. "Yet the September 11 attacks seem somehow different from the others, in a way that justifies a response different from those the United States has previously made to acts of terrorism" (*Harvard Law Review*, 2002: 1225). The questions raised by the editors of the *Harvard Law Review* were the following. Did 9/11 constitute an act of war (by a non-state actor) or did the American military become an instrument of criminal law enforcement? What was it about 9/11 that was different than earlier terrorist attacks such that a different response was called for? Granted that the damage to property and number of people killed was greater and that it, therefore, generated more counts of crime, was it also a different *kind* of crime? If so, what was different about 9/11 that caused the American approach to terrorism to change from multilateral negotiation and the use of international institutions, as with Pan American 103, to the unilateral development of policy that was announced and executed by the United States and its allies, including Canada? Granted "something" about the magnitude of 9/11 was involved in the shift, not just in the rhetoric but in the mechanics, from criminal justice to war. But, what?

The answer provided by the editors was that "the criminal law, which may once have seemed a sufficient mechanism for combating terrorism, may no longer appear adequate to the task" (*Harvard Law Review*, 2002: 1231). That is, the criminal-law system, whether national or international, is concerned with past conduct. The grave problem when confronting terrorism, and *a fortiori* suicide terrorists, is to prevent future attacks. This is especially true with pneumopathologically deformed terrorists seeking posthumous transfiguration for their actions (Cooper, 2004: ch. 4). Even more specifically, because those who actually executed the terrorist attack of 9/11 are dead and so beyond the reach of the law, the overriding interest of the United States is to punish those responsible, namely the al-Qaeda leadership and states that enable their activities. This overriding interest would not be met simply by arresting the individuals responsible. An acquittal, for example, of bin Laden before an international court would not discharge either the American (or, arguably, the Canadian) interest in punishment or in future safety. Because the justice system cannot guarantee punishment and future safety, it has been rejected "in favor of the sword." Accordingly, the United States "trusts the strength of its own arms more than the will of the international community" (*Harvard Law Review*, 2002: 1236). The overriding political reality that has conditioned the American response to 9/11 is therefore the demand for a one-to-one correlation between crime and punishment, as distinct from an ordinary and conventional insistence on due process and the strict adherence to the legal procedures of criminal law. Post 9/11, the objective of the law remains effective punishment and preventive action.

There is no implication that the demand for punishment has simply eclipsed the criminal law nor that privacy concerns are trumped and trampled by security ones. On the contrary: it means that counterterrorism legislation might best be understood as promoting, not derogating, the most basic rights—to life, liberty, and security of the person—that constitute a necessary condition for a sense of privacy (Cotler, 2002/03). It is probably fair to say, however, that most of the commentary on the statutory response by the Government of Canada has neglected both the actual context of the American response, namely the necessity of punishment, as well as the notion that security and privacy do not constitute a zero-sum game.

Bill C-36 & Its Critics

In the weeks following 9/11, lawyers in the Department of Justice in Ottawa worked long hours to prepare Bill C-36, the omnibus antiterrorism bill containing amendments to the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act, among others, as well as provisions respecting the registrations of charities, which organizations had become a subterranean way of financing terrorism (Bell, 2004a). C-36 was introduced on October 15. There followed in quick succession hearings before the House Justice and Human Rights Committee and a Spe-

cial Senate Committee. A few amendments were made and, almost as quickly as the USA Patriot Act, it became law on December 18, 2001.

Even before C-36 was passed, however, there arose immediate objections from lawyers, civil-liberties activists, and minority groups that C-36 amounted to an assault on the very basis of the Canadian constitution. Three weeks after C-36 was introduced, many of these critics gathered on short notice at the University of Toronto Law School to voice their misgivings (Daniels et al., 2001 contains the proceedings of this conference). Several of the participants later made very similar remarks before the Senate committee (see The University of Toronto, Faculty of Law, 2001; and associated URLs).

Many of the critics of C-36 used the occasion to give voice to some more or less focused anti-American sentiments. Others objected in principle to the notion that the Canadian "intelligence community," such as it is, should receive any increase in resources. A few critics analyzed the shortcomings of two specific and controversial provisions dealing with privacy and security: one concerned preventative arrests and the other investigative hearings. All these remarks are important, though for different reasons. The two former critical stances express sentiments that are remote from the political realities indicated by the actual American response to 9/11. The more focused and specific criticisms are more useful for an appraisal of Canadian antiterrorism legislation.

We begin with a consideration of the by-now formular anti-American position. Generally the argument begins by drawing an analogy with previous emergencies or crises. This is typically followed by a few isolationist remarks concerning the nobility of Canadian values and traditions and a lamentation that C-36 would mean an end to them, that it was passed in response to American demands, and that it must not become law without major changes.

Reg Whitaker, for example, drew a parallel between the Canadian response to 9/11 and the response made by Canada half a century earlier at the start of the Cold War when a Soviet cipher clerk, Igor Gouzenko, defected in Ottawa and explained to the RCMP the extent to which Soviet spies had infiltrated the military and security bureaucracies of Britain, the United States, and Canada. By so doing, Gouzenko also exposed the government of the day to some highly unwanted pressure. The wartime alliance with the Soviets had not yet publicly dissolved, and Prime Minister King had no intention of jeopardizing relations between the East and the West by making public the Soviet threat to Western security. Accordingly, his government systematically played down the report of the Commission of Inquiry, a secret tribunal that reported on the arrests and interrogations made pursuant to Gouzenko's information. "Others might draw strongly anti-Soviet lessons but Canada would not" (Whitaker, 2003a: 245). Whitaker's point, which was in fact overstated, was not that a similar pusillanimity has characterized many aspects of the Canadian response to 9/11 but that C-36 contemplated the creation of similar secret tribunals with unchecked power to compel confessions. As we shall see, this point was also overstated.

Whitaker went on to argue that even though Bill C-36, the Antiterrorism Act, and Bill C-55, the associated Public Safety Act, "disclose little that can be seen as directly responding to specifically American demands, as such, or reflecting American provisions and practices" nevertheless, Canada "was indeed forced" to change its aviation regulations to provide advanced production of itineraries and information on the method of payment for airline tickets for passengers arriving in the United States from Canada. He then added a common complaint, that this requirement by the Americans meant "overriding Canadian privacy law" but, like so many other privacy complainants, he provided no evidence that this was so, nor did he discuss in detail the contents of Canadian privacy legislation (Whitaker, 2003a: 258–59).

In a companion piece, Whitaker argued that 9/11 was simply an attack on the United States and thus not an attack on Canada, the West, and the civilized world. Canada, however, was compelled to respond because the United States did: "9/11 brought with it another kind of threat to Canada: collateral damage to Canadian economic security as a result of American national security concerns applied to the Canada-US border" (Whitaker, 2003b: 45). His conclusion seems to be that, trade aside, Canada has no national interest in joining any war on terrorists. This is highly questionable.

In his paper, "Did September 11 Change Everything? Struggling to Preserve Canadian Values in the Face of Terrorism," Kent Roach, a law professor at the University

of Toronto, like Whitaker, cited the Gouzenko case as an appropriate analogy as well as the internment and deportation of Japanese-Canadians after the 1941 attack on Pearl Harbor, the restrictive policy towards Jewish refugees from Nazi Germany, the use of the War Measures Act during the October crisis of 1970, and illegal acts of the RCMP around the same time. Roach was also aware that these analogies were largely unconnected with each other and overdrawn because "Bill C-36 does not contain provisions that authorize equivalent actions" but he thought the lack of similarity between these events and the passage of C-36 did not matter because "it is important that we be conscious of past overreactions in times of crisis" (Roach, 2001/02: 897). Roach was unconcerned that underreaction in times of war may well guarantee defeat.

Roach was, quite properly, critical of racial profiling (on anti-discrimination grounds rather than on grounds of ineffectiveness) and he was fully aware of the importance of surveillance of suspicious behaviour rather than trying first to establish and track identities (Roach, 2001/02, which cited Carter, 2001/02 favourably). He was even more concerned, however, with developing "a distinctive and moderate approach to antiterrorism measures" (898) By distinctive, Roach simply meant non-American; by moderate, he meant what his title suggests, that far from "changing everything" 9/11 did not change much so far as the struggle for "Canadian values" were concerned.

At two critical places in the development of his argument, Roach cited George Grant and Grant's reaction to the Cuban missile crisis of 1962 as a source of critical guidance on how to consider the implications of 9/11. "In my more pessimistic moments," he wrote,

> I find myself thinking of George Grant's famous *Lament for a Nation* in which he declares Canadian sovereignty and a distinctive Canadian democracy to be dead. That book was written in response to Canada's decision to accept nuclear arms in the wake of the Cuban Missile Crisis of 1962, an event that was more than the traumatic equal of September 11. My fear is that September 11 is driving us towards Americanized criminal justice and foreign policies that depart from Canadian values and traditions. In my more optimistic moments, however, I believe that it is too early, or perhaps just too futile, to lament a Canada that was lost on that surreal morning of September 11. We can and we must struggle to maintain a distinctive Canadian approach to the very real challenges posed by terrorism. (Roach, 2001/02: 898)

Roach did not indicate in any detail what he meant by "Americanized criminal justice and foreign policy" beyond its departure from "Canadian values and traditions." In fact, his concerns for "a Canada that was lost on that surreal morning of September 11" looks like nothing so much as an anxiety-inducing rhetorical trope.

Later in his essay he returned to George Grant and *Lament for a Nation*. The attack by al-Qaeda and the attempt by the Soviet Union to position ballistic missiles 90 miles away from Florida were both directed at the United States he said, but

> both events were traumatic for Canadians, discredited a Canadian nationalism that appeared anti-American, and led to a shift in Canadian policy towards closer co-operation with the Americans. The defeat of Prime Minister Diefenbaker in the 1963 federal election and the Liberals' acceptance of nuclear warheads for missiles in Canada led George Grant to write his famous *Lament for a Nation* declaring Canadian sovereignty and nationalism to be dead. (Roach, 2001/02: 935)

Roach then quoted from Grant's book, ending with the author's opinion that the Americans have no need "to incorporate us" because "a branch-plant satellite, which has shown in the past that it will not insist on any difficulties in foreign or defence policy, is a pleasant arrangement for one's northern frontier" (Grant, 1965: 86–87). Roach then commented:

> The pleasant arrangement contemplated by Grant was not so pleasant after September 11. The television version of the West Wing worried about terrorists crossing into the United States from Canada while the real West Wing authorized the tripling of its personnel on the ominously named "northern border." Given the increase in economic integration since Grant's time, this has placed enormous pressure on

> the Canadian government to co-operate with the Americans. And the irony has been that much of the Canadian co-operation and willingness to please the Americans has been directed not so much at the economic imperative of keeping the border open, but at issues of criminal justice and foreign policy. (Roach, 2001/02: 898)

Whatever one makes of George Grant (see Cooper, 1978; 1992), he had some very specific objections to make regarding American foreign policy (in Vietnam, for example) or about the importance of modern technology for thinking. In contrast, Roach's abstract and vague evocation of a "distinctive Canadian approach" to counterterrorism, namely the application of existing criminal law in support of "Canadian values and traditions" is not persuasive. As we have seen, criminal law is not enough.

Unfortunately, Roach is not alone. Wesley Pue, Professor of Law at the University of British Columbia, likewise advanced the opinion that, by following the American lead in combating terrorism, Canada is in a "new state of permanent war" (Pue, 2003: 292; see also Mia, 2003/04; Stuart, 2003/04; Paciocco, 2001). Because of this condition, he explained, "the knee-jerk reaction of security bureaucrats has been to move further in the preferred directions of concentrating power, constraining liberties, and enhancing both criminal justice and security bureaucracies" (Pue, 2003: 292). Mission creep is a real problem but Pue does not explain how far the mission has crept and what the changes mean for security and privacy.

In a similar vein, Whitaker argued that the Anti-Terrorism Act is

> actually a proto-National Security Act, most of the provisions of which have been in the pipeline in Ottawa for some time, many strongly favoured by elements within the security and intelligence community but stalled by the lack of attention paid to security and intelligence issues in pre-9/11 Ottawa. (Whitaker, 2003b: 57)

Whitaker then suggested that C-36 was simply an omnibus compendium of the "wish lists" of the various components of the Ottawa intelligence community and drew what is probably an accurate observation regarding the way bureaucratic politics is conducted in Canada: "The opportunity afforded by 9/11 was alertly seized by the security and intelligence community, which has ended up with much more than it would likely have achieved had 9/11 not happened" (Whitaker, 2003b: 58). Certainly one could make the same point regarding, for example, the "environmental community" and the opportunity provided by the Kyoto Protocol. In other words, there is invariably an element of opportunism in most legislative initiatives. That does not, however, make it objectionable (Wark, 2001). Whitaker's argument, however, was directed neither at the utility of the provisions of C-36 to the intelligence community nor whether some other package of provisions would be an improvement. What was particularly unfortunate, according to him, is that

> the atmosphere surrounding the specific elements of C-36's passage precluded an intelligent national debate on the merits of specific elements of C-36 that were not directly related to 9/11, especially its lack of any comprehensive review and oversight mechanisms for all the agencies involved. (Whitaker, 2003b: 58)

We will see, however, that such concern over a lack of oversight is exaggerated and, in any event, points to the dilemma of guarding the guardians rather than to a problem that might be solved by different words in the law.

Protecting the polity & its principles

Given this criticism of Bill C-36, it is useful to remind ourselves that free and democratic societies have both a common-sense right and a duty to protect themselves against terrorist attacks, other forms of asymmetric warfare, and ordinary criminals as well as to conduct traditional interstate warfare for the same purpose. At the same time, as critics of C-36 tirelessly observed, a free and democratic society cannot survive if it undermines its own constitutional principles. One of the most common ways of so doing is to transfer emergency powers into ordinary criminal law (Dyzehaus, 2001). One must, therefore, be mindful of the danger as well as of the purpose of antiterrorism legislation, namely to defend and protect the security and civil liberty of Canadians, not to diminish it.

Irwin Cotler has argued, correctly in my view, that C-36 should be considered first of all as "human security" legislation, which is to say legislation that supports the exercise of civil liberties and enables a sense of privacy (Cotler, 2002/03). According to him, something like C-36 is required by Canadian ratification of several United Nations Conventions on terrorism. However that may be, it is almost self-evident that, without security, civil liberties are not so much at risk as immediately threatened. To that end, Cotler, who at the time was an MP (he has since become Minister of Justice and Attorney General of Canada) on leave from the McGill Faculty of Law, elaborated 12 principles that sustain Bill C-36 as human security legislation, most of which can actually be found in the law.

In the second part of his paper, Cotler addressed concerns that had been raised by a number of civil-liberties lawyers about alleged threats to individual rights that were found in the original draft of C-36, some of which—dealing with the definition of a terrorist activity, *mens rea* requirements, sunset provisions, and the like—were addressed by amendments to the legislation. Other concerns, including some that arose from provisions of the Public Safety Act, Bill C-55, were not addressed.

This is not to say that reasonable people might not take issue with some of Cotler's concerns. For instance, s.4.82 of C-55 gives CSIS and the RCMP access to airline passenger lists. This does impinge on privacy inasmuch as the data may also be used by the police to identify individuals who have committed warrantable offences. Others may argue that this dual use of the data is a reasonable and proportional violation of a right guaranteed by the Charter. In any event, since neither C-55 nor C-36 was accompanied by the "constitutional override" or "notwithstanding" provision of s.33 of the Constitution Act, both laws are subject to Charter challenges.

C-36, Section 83.3—Recognizance with Conditions

As noted above, two provisions of C-36 have drawn a considerable amount of criticism (Trotter, 2001; Paciocco, 2001). The first, Section 83.3, provides for what are conventionally called "preventive arrests." Because terrorist attacks take place suddenly following a lengthy period of planning, the police and other law enforcement officials sought the power to arrest individuals prior to an actual incident. As Errol Mendes noted, "these are extraordinary provisions, which before September 11, 2001 would probably not have withstood a *Charter* challenge" (Mendes, 2002/03: 83). After 9/11, in Mendes' view, s.83.3 would meet all the provisions of the "Oakes Test," which establishes the criteria by which a Charter-based right can reasonably be limited in a free and democratic society. Moreover, "the consent of the Attorney General is required and the peace officer must satisfy a provincial court judge that there are reasonable grounds to believe that a terrorist activity will be carried out and that the arrest will prevent the carrying out of the terrorist activity" (Mendes, 2002/03: 89). Arguably, this procedure provides sufficient oversight.

Stanley Cohen, Senior General Counsel with the Department of Justice and understandably a supporter of the antiterrorism legislation, noted that the term, "preventive arrest" does not anywhere appear in C-36. The title of section 83.3 is "Recognizance with Conditions," and its purpose is not to arrest someone but to place someone under judicial supervision. Procedures to ensure recognizance with conditions are already part of the Criminal Code and are used chiefly in situations involving domestic violence and organized crime. They "enable a person to go to the court and ask for the imposition of conditions on another person because a legitimate, reasonable fear exists that the other person may commit an offence" (Cohen, 2002/03: 110). Once a person is brought before a judge, conditions may be imposed that do, indeed, restrict his or her freedom of movement or of association for the obvious purpose of simultaneously identifying and eliminating a threat. "Whether the exact mechanism the legislation provides is regarded as reasonable and proportional [and so meets the Oakes Test] will depend less upon its intrinsic substantive merit than upon the context in which it is used" (Cohen, 2003/04: 112). If it is used in the context of a terrorist threat, it would no doubt survive a Charter-based challenge.

C-36, Section 83.23—investigative hearings

Section 83.23 of Bill C-36 deals with investigative hearings. Here, with the consent of the Attorney General, a person may be brought before a judge and compelled to testify. Paciocco (2001) and Roach (2002/03) likened this procedure to the operations of the Courts of the Star

Chamber and High Commission (which also used torture as an interrogation tool and gave their inquisitors the task of determining guilt or innocence as well). It is true that the right to refuse to answer questions from the police is well entrenched in Canadian law so that compelled testimony is unusual. Even so, it does exist in securities law, coroners' inquests, and foreign criminal investigations undertaken within the framework of the MLAT, among other places. Moreover, the involvement of the Attorney General indicates that the procedure is a last, not a first, resort and, unlike the proceedings of the Star Chamber, C-36 contains extensive protections against self-incrimination, a right to legal counsel, and immunity from derivative prosecution.

It is worth recalling that the pressing and substantial objective of applying s.83.23 would again depend on the factual context, namely that a material witness provide information in a timely way to prevent the commission of a terrorist act. In other words, investigative hearings may in fact prevent security personnel from being tempted by more vigorous kinds of interrogation. Besides, as Cohen noted, this procedure is not designed to determine criminal liability but to gather evidence regarding a very specific and peculiar form of behaviour—and nothing else (Cohen, 2002/03). As a tool of investigation, the ability to compel testimony is similar to the procedures of an American grand jury (Mendes, 2002/03). We agree with the position of Wesley Wark:

> Investigative hearings and preventative detention are emergency measures, serious and ugly. But they have a practical role in preventing catastrophes, and focusing the minds of the security and intelligence community. They also send a signal to both the Canadian public and to our coalition allies in the war on terrorism. The signal is simple: Canada is serious. (Wark, 2001: 293)

Again, reasonable people can disagree about some of the provisions of C-36. Mendes, for instance, considered the oversight provisions to be inadequate but Cohen is of the view that they are sufficient to ensure that the act will be applied appropriately and thus contribute to the security of Canadians without undermining their rights to, or sense of, privacy. It is also worth noting that, in comparison to British, French, and American antiterrorism legislation, the Canadian acts provide much stronger safeguards (Mendes, 2002/03; Cotler, 2002/03). In short, if there are criticisms to be made of Canadian antiterrorism policy it is not in the area of the legal instruments. "It is worth remembering," wrote Wark, "that increased powers do not guarantee skillful execution" (Wark, 2001: 295). Indeed, even good laws may not be executed, which raises a final and broader question: the reluctance of the Canadian government to use the laws with which it has equipped itself.

Canadian reluctance to use antiterrorism legislation

The Auditor General, in her 2004 report to Parliament, discussed national security in Canada and the effectiveness of post-9/11 expenditures (see Canada, Auditor General 2004). The Auditor General's report, like the American *9/11 Commission Report*, drew attention to defects in the intelligence aspect of national security, the absence of any systematic catalogue of any "lessons learned," inconsistencies in watch-lists, lax security, especially on the "air side" at airports, and so on. Many of the Auditor General's observations also relate to the tension between security and privacy.

"The most significant issue still unresolved," she wrote, "is Customs officials' lack of access at the front line to information on lost and stolen passports" (Canada, Auditor General 2004: 17). Considering that an average of about 25,000 passports are lost or stolen each year, this is a serious problem. It is made worse by the fact that border watch-lists do not include information on lost and stolen passports. Instead, the Passport Office "deactivates" the document but "the information system used on the primary inspection line [that is, at a border crossing] cannot distinguish between active and deactivated passports" (Canada, Auditor General 2004: 31). Researchers in the Auditor General's office were told "that privacy concerns had to be overcome before the Passport Office could share the list of lost and stolen passports with Citizenship and Immigration" (Canada, Auditor General 2004: 31).

The Passport Office was not alone in citing "privacy concerns" as the reason why agencies did not share information. "However," the *Report* said, "officials were not

able to show us any legal opinions, specific references to legislation, or judgments as a basis for that position." In fact, "the Privacy Act accommodates the sharing of information among federal government agencies in a variety of situations, including for reasons of national security" (Canada, Auditor General 2004: 23). In short, the Auditor General argued that bureaucratic stonewalling, not genuine concerns over privacy, has blunted whatever antiterrorism tools are available in Canada.

Finally, it is worth noting that American officials have noticed the same defects in Canadian security practices as the Auditor General. Granted that most Canadians believe that 9/11 changed the world for the United States, it is also true as the arguments of Pue, Roach, or Trotter attest, that "only a tiny minority of Canadians believes that it likewise changed for Canada." Americans anticipate another attack from al-Qaeda; "Canadians have no comparable concerns—and that point irritates Americans"—not because they would prefer Islamist terrorists to attack the CN Tower or National Defence Headquarters, which as Whitaker said, would "send an indecipherable message to the world" (Whitaker, 2003a: 253), but because they think that Canada is not doing anything besides mouthing its concern, which "smacks of humouring that half-demented uncle who believes in alien abductions but has a sizeable legacy that you don't want to lose out on" (Jones, 2004: 7).

After a lengthy and detailed analysis of terrorist groups and networks in Canada, Stewart Bell reached the same conclusion, though he expressed it in less colourful language. Canada is an excellent staging area for terrorists, which is probably the main reason the country has not been attacked. There is a "security vacuum" that amounts to an open invitation to terrorists to enter the country and set up shop. "Canada's official terrorism policy—in effect denying there is a problem—is merely a public relations strategy intended to manage Washington in order to prevent the Americans from imposing border security measures that would slow North-South trade" (Bell, 2004a: A1).

Canada was fortunate in that none of the 9/11 terrorists entered America from this country. Even so, Americans do not believe that Ahmed Ressam, the "millennium bomber" apprehended by American authorities when he landed in Port Angeles, Washington on a ferry from Victoria, British Columbia en route to bomb Los Angeles International Airport, or the Khadr family, or the associates of Maher Arar, or the Jabarah brothers, Abdul Rahman and Mohamed Mansour, are "isolated weeds in a field of flowers" (see Bell, 2004b: A1). It is "disconcerting" to American authorities that 36,000 individuals who are subject to Canadian deportation orders are invisible, and even more disconcerting to them that most Canadians are unconcerned. Indeed, the refusal to locate—or even seriously attempt to locate—these individuals living in Canada illegally "suggests a lack of serious purpose gainsaying the ostensible commitment to shared security" (Jones, 2004: 8).

Finally, the hastily constructed National Security Policy, released shortly before the new Prime Minister visited Washington late in April 2004, did not seriously address the concerns that the Auditor General had published a month earlier (Moens, 2004; Canada, Privy Council, 2004). The annual terrorism report published by the American State Department was released the same day Paul Martin visited Washington. It gave a clear, albeit diplomatic account of Canadian terrorist policy: "As of November 2003, there were 34 organizations listed under the statute [The Anti-Terrorism Act] as entities engaging in terrorist activities. Although they are subject to prosecution under the Criminal Code of Canada, the law is untested since no prosecutions have taken place" (United States, Department of State, 2004: 8). As David Jones, a former US diplomat accredited to Ottawa noted "clearly our wavelengths are not in tune" (Jones, 2004: 8).

Conclusion

The initial concerns voiced by British Columbia's Information and Privacy Commissioner and amplified by local journalists concerned the extraterritorial application of the USA Patriot Act. We agree with the BC Attorney General that this is unlikely.

Broader reflection on the question of privacy and security led to the conclusion that there need be no conflict inasmuch as human security includes a sense of privacy. Or, to reverse the relationship, a lack of security can easily be manifest as a loss of privacy. At the same time, by analyzing the concept of security in terms of the distinction between behaviour and identity, it is clear that surveillance of behaviour enhances security without invading privacy. Determining identity on the basis of suspicious behaviour clearly does constitute an invasion of privacy for the very good reason that determining identity is intended to do just that. But this invasion of privacy was triggered by suspicious behaviour. There are no *prima facie* suspicious identities.

There are some legitimate concerns, based both on principle and on contemporary concerns over biometric surveillance technologies, that need to be discussed in greater detail by Canadian authorities. The objections to the two incarnations of TIA by American analysts could likely guide Canadian deliberations (Peña, 2002, 2003; Crewes, 2002a, 2002b).

Looking to Canadian antiterrorism legislation, and notwithstanding the somewhat abstract and exaggerated fears of some lawyers and other academic critics, the Canadian laws do contain checks against their arbitrary use by the executive. In this respect, the Canadian antiterrorism laws are probably superior to those of our traditional allies. At the same time, no law is perfect and bureaucrats, whether in or out of uniform, like other people, are likely to take advantage of every opportunity to make their own official lives easier.

If there are principled objections to be made to Canada's antiterrorism laws, they should be directed not against the legal instruments themselves but against the reluctance of the Government of Canada to use them. There is unquestionably a threat to the security of Canadians when greater emphasis is placed on Canadian "distinctiveness" than on effectiveness in mounting counterterrorism operations.

Privacy concerns are real but, in practice, they have become an excuse for bureaucratic inaction. By making the distinction between behaviour and identity and attributing greater weight to the former than the latter, there is, for example, simply no reason, besides bureaucratic stonewalling, to refuse to share information on stolen or lost passports with front-line inspectors. Someone who shows up with a stolen or lost passport at a border crossing point has already committed an offence and knows it.

We agree with Cotler that there is no necessary trade-off between security and privacy and that, on balance, Canadian antiterrorism laws meet the needs of security authorities, at least in theory. The enforcement of those laws, the actual practice of Canadian security policy, is something else. It may be a reflection of Canadian public opinion. If so, it may take a major breach of security in this country to awaken Canadians from their complacent slumbers.

References

Austin, Lisa (2001). "Is Privacy a Casualty of the War on Terrorism?" In Ronald J. Daniels, Patrick Macklen, and Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto, ON: University of Toronto Press): 251–67.

Bell, Stewart (2004a). *Cold Terror: How Canada Nurtures and Exports Terrorism around the World*. Toronto, ON: Wiley.

——— (2004b). "CSIS Reveals Exploits of Canadian Qaeda." *National Post* (August 26): A1.

Bowyer, Kevin W. (2004). "Face Recognition Technology: Security versus Privacy." *IEEE Technology and Society Magazine* 23, 1 (Spring): 9–20. <http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=28491&puNumber=44> (as of August 4, 2004).

Canada, Auditor General (2004). "National Security in Canada: The 2001 Anti-Terrorism Initiative." Chapter 2 in *Report of the Auditor General of Canada to the House of Commons* (March). Ottawa: Office of the Auditor General.

Canada, Privy Council (2004). *Securing an Open Society: Canada's National Security Policy*. Ottawa: Privy Council Office.

Carter, Ashton B. (2002). "The Architecture of Government in the Face of Terrorism." *International Security* 26, 3: 5–23. <http://80-muse.jhu.edu.ezpoxy.lvb.ucalgary.ca:2048/journals/internationalsecurity/v026/26.3carter.html> (as of August 9, 2004).

Center for Cognitive Liberty & Ethics [CCLE] (n.d.). "Cognitive Liberty and Mental Surveillance." <http://www.cognitiveliberty.org/issues/mental_surveillance.htm> (as of August 8, 2004).

Chachere, Vickie (2001). "Snooper Bowl? Biometrics Used at the Super Bowl to Detect Criminals in Crowd." *Associated Press* (February 13). <http://abcnews.go.com/sections/scitech/DailyNews/superbowl_biometrics_010213.html> (as of August 2, 2004).

Choudhry, Sujit (2001). "Protecting Equality in the Face of Terror: Ethnic and Racial Profiling and s.15 of the Charter." In Ronald J. Daniels, Patrick Macklen, and Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto, ON: University of Toronto Press): 367–81.

Choudhry, Sujit, and Kent Roach (2003). "Racial and Ethnic Profiling: Statutory Discretion, Constitutional Remedies, and Democratic Accountability." *Osgoode Hall Law Journal* 41, 1: 1–36.

Cohen, Stanley A. (2002/03). "Safeguards in and Justification for Canada's New Anti-Terrorism Act." *National Journal of Constitutional Law* 14: 99–124.

Cooper, Barry (1978). "Ab Imperio usque ad Imperium: The Politics of George Grant." In Larry Schmidt, ed., *George Grant in Process: Essays and Conversations* (Toronto, ON: Anansi): 22–39.

——— (1992). "Did George Grant's Canada Ever Exist?" In Y.K. Umar, ed., *George Grant and the Future of Canada* (Calgary, AB: University of Calgary Press): 151–64.

——— (2002). "Unholy Terror: The Origin and Significance of Contemporary, Religion-based Terrorism." Studies in Defence & Foreign Policy, Number 1 (May). Vancouver, BC: The Fraser Institute.

——— (2004). *New Political Religions, or an Analysis of Modern Terrorism*. Columbia, MO: University of Missouri Press.

Cotler, Irwin (2002/03). "Terrorism, Security, and Rights: The Dilemma of Democracies." *National Journal of Constitutional Law* 14: 13–69.

Crewes, Clyde Wayne Jr. (2002a). *Human Bar Code: Monitoring Biometric Technologies in a Free Society*. Policy Analysis 452 (September 17). Washington, DC: The Cato Institute. <http://www.cato.org/pubs/pas/pa-452es.html> (as of September 27, 2004).

——— (2002b). *The Chill from the Pentagon*. Washington, DC: The Cato Institute. <http://www.cato.org/research/articles/crews-021125.html> (as of September 27, 2004). Originally published on *National Review Online* (November 25, 2002).

———. (2003). *The Poindexter Awareness Office: Turning the Tables on Mr. Supersnoop*. <http://www.cato.org/dailys/01-15-03.html> (as of September 27, 2004). Originally published in the *Orange County Register* (January 5, 2003).

Daniels, Ronald J., Patrick Macklen, and Kent Roach, eds. (2001). *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. Toronto, ON: University of Toronto Press.

Demchak, Chris, and Kurt D. Fenstermacher (2004a). "Balancing Security and Privacy in the 21st Century." In H. Chen, R. Moore, and D. Zeng, eds., *Intelligence and Security Informatics* (Tucson, AZ: Springer).

——— (2004b). "Balancing Security and Privacy in the Information and Terrorism Age: Distinguishing Behavior from Identity Institutionally and Technologically." *The Forum* 2, 2: Article 6. <http://www.bepress.com/forum/vol2/iss2/art6>.

Dyzehaus, D. (2001). "The Permanence of the Temporary: Can Emergency Powers Be Normalized." In R.J. Daniels et al., eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto, ON: University of Toronto Press): 21–38.

Grant, George (1965). *Lament for a Nation: The Defeat of Canadian Nationalism*. Toronto, ON: McLelland & Stewart.

Grossman, L. (2001). "Welcome to the Snooper Bowl." *Time* (February 12): 57.

Hansard (2001). Statement by Justice Minister, Anne McLelland, *House of Commons Debates*, vol. 137, no. 80, 1st Session, 37th Parliament, 18 September, p. 5220.

Harper, Jim (2004). *Understanding Privacy—and the Real Threats to It*. Policy Analysis 520 (August 4). Washington, DC: The Cato Institute. <http://www.cato.org/pubs/pas/pa-520es.html> (as September 28, 2004).

Harvard Law Review (2002). "Responding to Terrorism: Crime, Punishment, and War." *Harvard Law Review* 115, 4: 1217–38.

Jones, David T. (2004). "When Security Trumps Economics: The New Template of Canada-US Relations." *Policy Options* (June/July): 73–78.

Kines, Lindsay (2004). "BC Drafts Privacy Law to Curb US Patriot Act." *The Vancouver Sun* (July 24): A1.

Kirsch, Steve (2001). *Identifying Terrorists before They Strike by Using Computerized Knowledge Assessment (CKA)*. <http://www.skirsch.com/politics/plane/ultimate.htm> (as of August 8, 2004).

Mendes, Errol P. (2002/03). "Between Crime and War: Terrorism, Democracy and the Constitution." *National Journal of Constitutional Law* 14: 71–97.

Mia, Ziyaad E. (2003/04). "Terrorizing the Rule of Law: Implications of the Anti-Terrorism Act." *National Journal of Constitutional Law* 14: 125–52.

Moens, Alexander (2004). "Canada's National Security Strategy and NATO's Response Force." *Fraser Forum* (May): 13–15.

Paciocco, David M. (2001). "Constitutional Casualties of September 11: Limiting the Legacy of the Anti-terrorism Act." *The Supreme Court Law Review* 16: 185–237.

Palmer, Vaughn (2004). "No Nosy US Patriot Act Here, Thanks." *The Vancouver Sun* (July 24): A3.

Peña, Charles V. (2002). *Total Information Awareness: Back to the Future*. Washington, DC: The Cato Institute. <http://www.cato.org/dailys/12-07-02.html> (as of August 10, 2004).

——— (2003). "TIA Redux: Still Bad Math." Washington, DC: The Cato Institute. <http://www.cato.org/dailys/06-05-03.html> (as of August 10, 2004).

Province of British Columbia (2004). *Submission to the Information and Privacy Commissioner for British Columbia: Examination of USA PATRIOT ACT Implications for Personal Information of British Columbia Residents Involved in Outsourcing of Government Services to US-linked Service Providers* (July 23). <http://www.gov.bc.ca/mser/down/submission.pdf> (as of August 10, 2004).

Pue, W. Wesley (2003). "The War on Terror: Constitutional Governance in a State of Permanent Warfare:" *Osgoode Hall Law Journal* 41: 267–92.

Roach, Kent (2001/02). "Did September 11 Change Everything? Struggling to Preserve Canadian Values in the Face of Terrorism." *McGill Law Journal* 47: 893–947.

Snow, Thomas G. (2002). "The Investigation and Prosecution of White Collar Crime: International Challenges and Legal Tools Available to Address Them." *William and Mary Bill of Rights Journal* 11: 209–33.

Stuart, Don (2003/04). "The Anti-Terrorism Bill C-36: An Unnecessary Law and Order Quick Fix that Permanently Stains the Canadian Criminal Justice System." *National Journal of Constitutional Law* 14: 153–66.

The University of Toronto, Faculty of Law (2001). The Security of Freedom: A Conference on Canada's Anti-Terrorism Bill (November 9–10). <http://www.law.utoronto.ca/c-36/history.htm> (as of August 4, 2004).

Toobin, Jeffrey (2001). "Crackdown." *The New Yorker* (November 5): 37–41.

Trotter, G. (2001). "The Anti-terrorism Bill and the Preventative Restraints on Liberty." In Ronald J. Daniels et al., eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto, ON: University of Toronto Press): 239–48.

United States, Department of State (2004). *Patterns of Global Terrorism 2003*. Washington, DC: US State Department.

United States, House of Representatives (2001). Bill, H.R 3162. *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.* 107th Congress, 1st Session, 2001 (enacted). <http://www.fincen.gov/hr3162.pdf> (as of October 4, 2004).

United States Senate (1988). *Senate Treaty Documents*, 100–114. 100th Congress, 2nd Session, February 22.

Volokh, Eugene (2002). "Big Brother is Watching—Be Grateful!" *Wall Street Journal* (March 26): A22.

Wark, Wesley (2001). "Intelligence Requirements and Anti-terrorism Legislation." In Ronald J. Daniels et al., eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto, ON: University of Toronto Press): 287–96.

Weiser, Benjamin (2001). "Four Guilty in Terror Bombings of Two US Embassies in Africa." *New York Times* (May 30): A1.

Whitaker, Reg (2003a). "Keeping Up with the Neighbours? Canadian Responses to 9/11 in Historical and Comparative Context." *Osgoode Hall Law Journal* 41: 241–65.

——— (2003b). "More or Less than Meets the Eye? The New National Security Agenda." In G. Bruce Doern, ed., *How Ottawa Spends: 2003-2004: Regime Change and Policy Shift* (Toronto, ON: Oxford University Press): 44–58.

Woodward, John D. Jr. (2001). *Super Bowl Surveillance: Facing up to Biometrics*. Santa Monica, CA: RAND. <http://www.rand.org/publications/IP/IP209/IP209.pdf> (as of August 4, 2004).

Zhao, W., R. Chellappa, P.J. Phillips, and A. Rosenfeld (2003). "Face Recognition: A Literature Survey." *ACM Computing Surveys* 35, 4: 399–458. <http://portal.acm.org/citation.cfm?doid=954342> (as of August 2, 2004).

About the Author & Acknowledgements

Barry Cooper is Senior Fellow and Managing Director of the Alberta Policy Research Centre of the Fraser Institute, Professor of Political Science at the University of Calgary, and a Fellow of the Centre for Military and Strategic Studies. He has has written and lectured extensively on terrorism and associated security issues, political philosophy and Canadian public policy. His recent publications for The Fraser Institute include *Canada's Military Posture: An Analysis of Recent Civilian Reports* (with Mercedes Stephenson and Ray Szeto); *Policing Alberta: An Analysis of the Alternatives to the Federal Provision of Police Services* (with Royce Koop); *Unholy Terror: The Origin and Significance of Contemporary, Religion-based Terrorism*; and "North American Military Relations: How Can Canada Help?" (*Fraser Forum*, June 2004). He has received the Konrad Adenauer Award from the Alexander von Humbolt Stiftung and a Killam Research Fellowship. He is a Fellow of the Royal Society of Canada.

Acknowledgments

The author would like to thank Gillian Frank, Brian Purdy, and Martin Collacott for their helpful comments on an earlier version of this paper.