Human Rights in the Global Village: The Challenges of Privacy and National Security

Professor A. Wayne MacKay[1]
Professor of Law, Dalhousie University
Vice Chair, International Center for Human Rights and Democratic Development

I. Introduction: Privacy and National Security in Canada's Global Village

In the 1960's renowned Canadian academic, Marshall McLuhan, coined the term "global village." McLuhan's vision of the global village was that the world was a community in which distance and isolation had been dramatically reduced by electronic media. In the global village we are crossing borders physically, with travel and trade, and we're also crossing borders virtually with technology, like the phone and internet. There are many benefits to living in the global village but there are also casualties of this new world order, and one of them is privacy.

International human rights and domestic human rights are increasingly related in the global village. What we do in Canada affects the rest of the world and our actions have worldwide implications. Similarly, actions outside Canada's borders can and do have an impact here. Canada has an obligation to provide a model; we need to stand straight lest we cast a crooked shadow. Canada has tried to live up to this obligation. For example, Canada was a leader in the 2005 Southeast Asia tsunami relief. Also in 2005, then Prime Minister Martin, took a stand on anti-ballistic missile defense and let the world know that Canada would not be involved, albeit not as quickly as some would have liked.

I commend to interested world observers, Lloyd Axworthy's *Navigating a New World: Canada's Global Future*. This thoughtful exploration of Canada's role in the modern world recognizes the strong influence of nationalism even in an increasingly integrated "global village."

The global village is becoming a trifle overcrowded. The streets teem with close to 190 nations. The big and powerful strut and swagger at center stage, while the poor and small are shuffled to the outer edge. Others are states in name only, presiding over a presidential palace while a group of warlords control the hinterlands. Yet national

[1] Professor MacKay would like to acknowledge the research and earlier drafting assistance of Megan Leslie, legal worker at Dalhousie Legal Aid, Halifax and the proof reading of Michael Fenrick, second year Dalhousie Law student, and prospective graduate of 2008.

sovereignty is still acknowledged to be the right of each villager, even though the reality is that all the inhabitants find their fortunes intertwined.

The world has changed since the World Trade Centre terrorist attacks of September 11, 2001, and this leaves us with questions about what kind of model Canada wants to embrace in regards to privacy and security. Is Canada willing to sacrifice certain human rights to ensure a secure world after September 11? How much of our privacy are we willing to give up to ensure that we're safe? These issues have been re-emphasized by the terrorist bombings in the London subways in July, 2005, and, more recently, by events in Canada.

On June 3, 2006, Canada had a direct brush with the terrorist threat when 17 people allegedly planning an imminent strike in Ontario were arrested by police and security forces. The security sting operation was complex and is shrouded in secrecy, as agents had to sign confidentiality statements under the Official Secrets Act. Targets of the alleged plot included political and economic symbols such as, the Parliament Buildings, the Peace Tower, CN Tower and the Toronto Stock Exchange. There were also reported plans to behead the Prime Minister, take other politicians hostage and storm the CBC and use it for communication.

After two years of surveillance the pre-emptive arrests were made in a sting operation whereby the alleged terrorists attempted to purchase fertilizers with ammonium nitrates (suitable for making bombs) in quantities three times larger than those used by the bombers in the 1995 Oklahoma City bombing (1 tonne was used there). The Oklahoma bombing resulted in the death of more than 150 people. It would appear that the 17 suspects were Canadians of Islamic faith and this raises concerns, about both a backlash and racial profiling, which I will discuss later. There is no doubt that the prompt and effective action of the police and security forces may have averted disaster and human tragedy. How this result was achieved is not yet known. This event does make clear that terrorist threats are still very real five years after planes flew into the World Trade Center and that Canadians are not immune.

It has become cliché to say that these events - described in short hand terms as "9/11" - changed the world. This is only partly true, as terrorism has been an international force for many years. However, on September 11, 2001 the reality of terrorism was visited on the heartland of the United States and it became clear to all that even a super power was vulnerable to the forces of terrorism afoot in the world. The world may not really have changed as a result of "9/11", but the way that the United States, and by association Canada, approach the world did. We have become more cautious and national security has become a value that trumps most other values – including human rights.

There is no doubt that “9/11” was one of those catastrophic events that enters our consciousness. Most people can tell you what they were doing when the planes crashed into New York’s twin towers on September 11, 2001. Personally I was in Duggers’ Mens’ Wear on Spring Garden Road in Halifax with my spouse, JoAnn, purchasing a suit and watching the horrific scene on the television in the store. I had recently been appointed as President of Mount Allison University in Sackville, New Brunswick and I had a meeting on university funding (along with many other Atlantic university presidents) with then Prime Minister, Jean Chretien, and his officials later in the day. Needless to say, the meeting was cancelled as the Prime Minister attended to the more pressing events of the day.

Later that same fall on October 24, 2001, I appeared as an expert witness before the Special Senate Committee on Bill C-36, (Canada’s proposed Anti-Terrorism Act) and made a presentation under the title of “Security at What Price?” My argument was that a total surrender of civil liberties in the name of national security would be allowing the terrorists to defeat democracy in a different way. Other witnesses before this Committee raised similar concerns. It is reassuring that Canada engaged in a more extensive and robust debate about balancing human rights and national security than the United States did when it enacted the Homeland Security Act and the Patriot Act. Again on March 15, 2005 I appeared before the Special Senate Committee Reviewing the Anti-Terrorism Act and made a presentation entitled “Human Rights and Counter Terrorism: A Fine Balance.” I emphasized that the burden was on the Government to demonstrably justify the need for the special investigative powers of the Act in order to justify its limitations upon basic rights; such as, fair process and privacy. Concerns were also raised by me and other witnesses, about the dangers of racial profiling. It will be interesting to see what effect the recent Ontario arrests will have upon this debate and whether it will dampen any appetite for revising the Anti-Terrorism Act.

Before turning to privacy in the context of terrorism, I will first examine privacy in the Canadian context, and secondly privacy as a human right. Freedom of the individual is a fundamental value held by democratic societies. Each person should have maximum personal autonomy but freedom of the individual needs limitations. Pursuing absolute freedom can result in harm to others. For example, freedom of the individual does not include the right to kill or express oneself in a violent way. If it did, then the victim’s freedom would be severely restricted. The existence of freedom requires restrictions. In this new age of terrorist threats we must look at what is sacrificed in the name of national security.

We need to consider what laws are required to protect our rights and freedoms, while still giving us the greatest possible security. There is a distinction between human rights, which require state intervention, and civil liberties, which require freedom from state intervention. If we believe that privacy is a human right then positive action is

required – we need to take positive action to protect it. This explains the growth in statutes at both federal and provincial levels aimed at protecting privacy and personal information. The balance is, in part, the relationship between freedom and equality. It is also an important part of drawing the proper line between the promotion of security in an unstable world and the protection of privacy. Privacy is one of the first casualties of the war on terror.

Constitutional Right to Privacy

Is privacy a human right? And if it is, how do we, and should we, protect it? In the United Nations' Universal Declaration of Human Rights Article 3 reads: "Everyone has the right to life, liberty and the security of person." Article 12 further stipulates:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Here at home in Canada, some of the language of article 3 appears in the Canadian Charter of Rights and Freedoms, a part of our Constitution, but there is no real equivalent to Article 12 in either the Charter or other privacy legislation. The only human rights code exception is in Quebec, where privacy is a matter for the Quebec Charter of Rights. The Quebec Charter states that every person has a right to respect for his private life; otherwise, there is not a clear statutory right to privacy in Canada.

There is legislation, however, such as privacy acts or protection of privacy statutes; but even these statutory protections are more concerned with access to information and controlling its flow, than guaranteeing a zone of privacy. What is typical of this kind of legislation is that privacy protection is more about controlling information rather than creating an umbrella of privacy protection. Privacy and access to personal information are the flip sides of each other. In Canada the law of privacy is generally about control over personal information, rather than privacy in broader terms of being left alone, like we see in the Universal Declaration of Human Rights. One aspect of privacy is access to information about yourself held by either the State or private agencies. This is an important aspect of privacy in the context of criminal law and accusations of terrorism. A veil of secrecy surrounds national security and a person often cannot get access to the evidence against him or her.

When we look to the Canadian Constitution we find that the constitutional protection of privacy in Canada is ill-defined and limited. Section 8 of the Canadian Charter of Rights and Freedoms reads: "Everyone has the right to be secure against unreasonable search or seizure."

This section has been interpreted to include a reasonable expectation of privacy. What does reasonable mean? A case at the Ontario Court of Appeal found that surveillance cameras in a public washroom weren't a violation of section 8, because the washroom was a public area. In another case the Supreme Court of Canada found that videotaping in a private hotel room was a violation of section 8 and that there was a reasonable expectation of privacy in a private hotel room.

The section 8 right against unreasonable search and seizure also relates to the human body. In another Supreme Court of Canada case the Court found that using bodily substances for unintended purposes violated one's personal autonomy, and that a violation of the sanctity of a person's body is much more serious than a violation of one's office or home.

Privacy can also be violated by allowing access to personal information for purpose beyond those that were originally intended. One example of this is R. v. Plant where the police were able to charge the accused suspects for operating a marijuana "grow-op" by getting access to their electricity records – which revealed unusually high use. More recently in R. v. Tessling the Supreme Court of Canada upheld the use of infra-red aerial photography to penetrate the walls of a house. This was held not to violate section 8 of the Canadian Charter, even though the United States Supreme Court did find a constitutional violation in a similar context. The critical factor for Canada's Supreme Court was the categorization of the invasion of privacy as being one of informational privacy, rather than personal or territorial. At the Ontario Court of Appeal level in Tessling, Justice Rosalie Abella regarded the privacy invasion as territorial and found that the breach of the sanctity of the home did produce a violation of section 8 of the Charter. She was overturned by the Supreme Court upon which she now sits.

The critical question in cases dealing with section 8 of the Charter is what constitutes a reasonable expectation of privacy in different contexts. In the rather unusual case of R. v. Belnavis the majority of the Supreme Court of Canada held that a passenger in a vehicle had a lower expectation of privacy than the driver in respect to a police search. In a spirited dissent, Justice LaForest disagreed with the majority opinion of Justice Cory and concluded that the emphasis should be more upon the person and his/her expectation of privacy and less upon who controlled the place or territory, in this case the automobile. A similar approach, focusing on the control of the physical territory, was taken in R. v. Edwards concerning the search of the possessions of a boyfriend who occupied but did not rent his girlfriend's apartment. Justice LaForest, who has been a consistent champion of privacy rights, stressed the need to focus on the person rather than the place but his was not the majority view.

Section 7 of the Charter has not been consistently interpreted by the courts as encompassing the substantive right to privacy. Section 7 reads: "Everyone has the right

to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."

The Supreme Court of Canada has stated that in the criminal context, section 7 extends beyond protection against arbitrary arrest and detention, and that generally speaking, the right to security of the person must include some protection from state interference when a person's life or health is in danger. Every instance of video surveillance, blood testing or genetic testing has the potential to endanger a person's life or quality of life by exposing the most private information about that person.

Although in the past, section 7 of the Charter has not consistently been interpreted by the courts as encompassing the substantive right to privacy, recently there has been a tendency to include such a right under not only section 8 but also section 7. The Court has said that section 7 is concerned not only with physical liberty, but also with "fundamental concepts of human dignity, individual autonomy, and privacy."

Case law has given us a very broad definition of privacy. In a case called R. v. Dyment Supreme Court Justice LaForest wrote:

> …society has come to realize that privacy is at the heart of liberty in a modern state…grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.

Claims to privacy must, of course, be balanced against other societal needs, and in particular law enforcement, and that is what s. 8 intended to achieve.

This case identified three categories of privacy: privacy related to place, privacy related to the person, and privacy that arises in the information context. Privacy in relation to information is based on the notion of the dignity and integrity of the individual, but how can we protect our privacy, and, therefore, our dignity and integrity, when we are faced with a global village where information can be transferred across borders with a click of a button? To quote Justice LaForest further, from the Dyment case,

> Retention of information about oneself is extremely important. We may, for one reason or another, wish to be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected.

There is some indication that the Supreme Court of Canada is open to an expanded concept of section 7 of the Charter but the situation is far from clear. The original 1980 draft of the Charter included protection from “arbitrary or unlawful interference with privacy” – language that is reminiscent of Article 12 of the Universal Declaration of Human Rights. This wording was deleted from the final version of the Charter. Thus it is not surprising that the major constitutional protection of privacy comes in the form of section 8 rather than section 7. Even the protection of privacy under section 8 depends heavily on the context.

Statutory Rights to Privacy

With such vague definitions of privacy it can be complicated trying to determine what a violation of privacy is and what it is not. Under certain federal privacy legislation if you suspect that your privacy has been violated by federal officials, you can make a complaint to the Privacy Commissioner. There are similar kinds of offices in most provinces, although the extent of their powers varies. The federal Office of the Privacy Commissioner publishes case summaries of investigated complaints online.

As an example, in one summary, the federal Privacy Commissioner investigated an employee complaint that the person’s employer was forcing them to consent to giving their voice print for the purpose of accessing a number of the company’s business applications. The company stated that this system offered the highest level of security for customer data, that it was very efficient and very cost effective. The Commissioner found that the voice print was an encroachment upon the person’s privacy, because the company was collecting the behavioural and physical characteristics that make an individual’s voice unique. However, she also found that the voice print did not really reveal much information about the individual. The employer’s needs thus outweighed the employee’s right to privacy.

What does this say about privacy in Canada? As we have seen, Canada has safeguards to protect privacy at both federal and provincial levels, but they are mostly concerning access to and control of information. This is true of the Personal Information Protection and Electronic Documents Act (PIPEDA) which does extend some privacy protection to the private as well as the public sphere. Access to information, including personal information about yourself, is a vital aspect of privacy in the context of issues of national security as I will examine shortly. We should know what the State knows about us. Canadians are pretty tolerant of the State prying into our lives and accepting of limits upon privacy, so long as we are given the context and good reasons for the limitations. This was the situation even before the post-“9/11” world with its constant threat of terrorism. However, control over our own personal information is a critical element of individual autonomy.

II. National Security and Privacy in the Context of Terrorism

Now that I have considered the definition of privacy in the Canadian context, let us consider the issue of national security and privacy in the context of terrorism. I will explore the broad definition of terrorism in the Anti-Terrorism Act, followed by a discussion of racial profiling in Canada.

Racial profiling has been defined as "any action undertaken for reasons of safety, security or public protection that relies on stereotypes about race, colour, ethnicity, ancestry, religion, or place of origin, rather than on reasonable suspicion, to single out an individual for greater scrutiny or different treatment." Before September 11 the issue of racial profiling in Canada, at both a domestic and international level, was described as the crime of "driving while Black." To illustrate this consider the example of boxer Kirk Johnson's case in front of the Nova Scotia Human Rights Tribunal. When Mr. Johnson was pulled over by police in his expensive car with Texas license plates, the Tribunal found that race was a determining factor. Since September 11, the phrase "driving while Black" has been recoined as "flying while Arab." "Profiling" is broader than just race now – it takes account of religion and culture, and even ideology. Perhaps we should talk about "profiling" and not just "racial profiling."

Concerns about profiling based on race, culture or religion are real and accentuated by threats of terror. The day after the arrests of 17 terrorist suspects in Ontario, windows were broken in an Islamic mosque in Toronto. There is an alarming tendency to paint a whole group with one brush, when in fact it is the acts of individuals, rather than religious or ethnic groups that are at fault. To its credit, the editorial in the Toronto Globe and Mail following the damage to the mosque, made a strong plea for tolerance, which I will quote at length. This editorial reads as follows:

Here? In Canada? Right in our midst? The dread of the enemy within is one of the most powerful any society can confront. News that authorities have broken up a suspected terrorist conspiracy in Ontario is bound to stir such fears. Some will even leap to the conclusion that our experiment with mass immigration and multiculturalism is falling, that our very tolerance and openness have become a weakness. That would be both rash and unjustified. Though Canadians are right to be alarmed at the weekend's news, it would be tragic if this incident made them question this country's greatest virtues.

There is nothing to indicate that Canada is riddled with extremists or that our practice of welcoming newcomers has made us a special target. The number of suspects arrested in the alleged plot to attack targets in Southern Ontario is 17. The number of Muslims living in Canada is 750,000. The vast majority of them are law-abiding and peace-loving. Most have integrated or are becoming integrated into the broader society, just as waves of immigrants from other lands and religions have done. To paint them all with

the same brush, as some bigots appear to have done when they vandalized a Toronto mosque on the weekend, would be shamefully un-Canadian.

For reasons that are not clearly understood, but demand to be, a small number of Muslim Canadians appear to be attracted to the hateful creed preached by Osama bin Laden and his ilk. If initial indications are correct, most of those arrested on Friday on terrorist charges are “homegrown” terrorists, established residents of this country, not foreign infiltrators. We need to know much about how they succumbed to this odious ideology. Were they converted to it by radical imams? Were they seduced by internet propaganda? Where did their resentment come from, in a land as welcoming and respectful as Canada?

Whatever the answer, there is nothing to suggest they are remotely representative. Nor is there any sign that some sin that Canada committed, either by excluding them, or by accepting them too uncritically, led them to do what they are said to have done.

Our American neighbours have raised concerns ever since September 11, 2001, that Canada may be a haven for terrorists. While the effective response of Canadian police forces in 2006 has been praised, fears of Canada as a terrorist soft spot on the northern border have been rekindled. Debates about immigration policy and multi-culturalism will also continue in the context of a real terrorist threat. It should also be noted that the police and security forces went out of their way to emphasize that the actions were those of individuals and not a particular cultural or religious group. This is an encouraging start.

Definition of Terrorism

Profiling is more accepted and widespread in the United States but that is not to say that it does not also happen in Canada. It is also an issue here at home. Nonetheless, anti-terrorism legislation in Canada is silent on the issue of discrimination. There is no anti-discrimination provision in the legislation, however the broad definition of terrorism, as added to the Criminal Code by the Anti-Terrorism Act, facilitates group profiling.

Canada’s Criminal Code defines terrorist activity as an act or omission that is committed in whole or in part for a political, religious or ideological purpose, objective or cause, with the intention of intimidating the public, with regard to its security, including economic security. The act or omission must intentionally cause death or serious bodily harm, endanger a person’s life, cause risk to the health or safety of the public, cause substantial property damage, or cause serious interference with or serious disruption of an essential service, facility or system. The key point here is that the definition includes motivational factors; the activity must be for political, religious or ideological reasons. The effect is that this piece of legislation creates statutory profiling. This may not have been the intent but it is the result.

Former Justice Minister, Irwin Cotler, supported the idea of removing the motivational factors from the definition in an article he wrote for the National Journal of Constitutional Law, written when he was a professor of law. The motivational factors could also be countered by a non-discrimination clause, for example, " for greater certainty, the expression of a political, religious or ideological thought, belief or opinion does not come within the definition of paragraph (b) of the definition "terrorist activity" in subsection (1) unless it constitutes an act or omission that satisfies the criteria of that paragraph." Clearly the effect of the Act would be the same, penalizing intimidation, intentional violence, etc., with the addition of this clause. However the anti-discrimination clause would take a needed step toward ensuring that the Act not be used for discriminatory purposes. To quote Cotler:

> at a time when fear tends to overcome rationality and risks prompting certain otherwise unthinkable assumptions and finger-pointing towards those perceived as threatening, particular vigilance is imperative in ensuring the protection of minorities. It is hoped that the special training being given to law enforcement authorities respecting the singling out of minorities in the administration of criminal justice may help to address these concerns.

The early response of the police in the recent Ontario arrests offers some signs of hope that sensitivity will prevail in these matters.

Despite the statutorily condoned profiling of this legislation, there is state protection for minorities in the form of other legislation, for example, the hate provisions of the Criminal Code that are expanded in the Anti-Terrorism Act. Section 320.1 of the Code states that if there are reasonable grounds to believe that hate material is on a computer, it can be ordered that the material be produced or deleted. The grounds of hate in this case are religion, race, colour, ethnicity and nationality. Section 430 (4.1) adds "religious property damage" to the offence of mischief as well, but Cotler suggests that this should be amended to explicitly include all other identifiable community institutions such as schools, cemeteries and community organizations, rather than focusing only on religion.

Nevertheless, the breadth of the definition of terrorist activity is still a problem. It includes conspiracy, attempt, threat, accessory after the fact, counseling, and facilitation. While something similar has not yet happened in Canada, in the US radical lawyer, Lynn Stewart, was charged under their laws on terror, for releasing a statement from a jailed terrorist. Under US anti-terrorism law Ms. Stewart was convicted for materially supporting a convicted terrorist and for knowingly abetting his murderous ambitions. Is it possible that the same thing could happen here at home?

How does Canada deal with security in the context of terrorism when keeping Canada safe means deporting someone to a country where they may be tortured? In a Supreme Court of Canada case called Suresh, the Canadian government had determined that a man who was a refugee from Sri Lanka was a member and fundraiser for the Liberation Tigers of Tamil Eelam, an organization alleged to be engaged in terrorist activity in Sri Lanka. While it would have been simple enough just to deport Suresh to Sri Lanka, deportation would have put him at risk of torture. Torture, whether we commit the act in Canada or send someone to it in another country, might violate his Charter right to life, liberty and security, and deportation to torture may be contrary to both the Charter and international law. The Court heard the argument that the terms “terrorism” and “danger to the security of Canada” as defined by the Immigration Act, were too vague, but held that they were not unconstitutionally vague.

Mr. Harkat, aged thirty seven has been held in various Canadian jails for more than the last three years, while he fought an order deporting him to Algeria, where he claims that he will be tortured. Pending this challenge being heard in the June, 2006 Supreme Court of Canada hearing, Mr. Harkat will be free on strict bail conditions, which include constantly wearing an electronic tracking bracelet., not using a computer and only using a telephone line that is monitored by authorities. He was detained for possible terrorist activities shortly after September 11, 2001 along with some other Muslims. Hr Harkat is not a Canadian citizen and was detained on the basis of a “security certificate” which I will explain more fully shortly.

Under these certificates he is deemed to be a security threat to Canada, but the Federal Court at both the trial and appeal levels held that being on bail with strict conditions does not pose a security threat, even though he was found to have been engaged in terrorist activities on behalf of Al-Qaeda. The upholding of his release on bail and his imminent release from jail has caused considerable stir in the wake of the June arrest of seventeen suspected terrorists in Ontario. His bail conditions sensibly restrict his freedom and privacy but some Canadians would prefer that he were kept in jail. It will be interesting to see what the Supreme Court of Canada will have to say about the merits of his constitutional claims against his detention as a security threat. This will be an important Charter test of where the line should be drawn between rights and national security. It is also interesting to note that the bail hearings for the seventeen suspected terrorists arrested in June, 2006 will be subject to a media ban and take place behind closed doors.

This is another example of Canada trying to strike a balance between combating terrorism and a person’s rights. The Suresh case was about process – he wasn’t given the proper procedural safeguards and the case was sent back to the Minister to do it again. There were found to be no problems with the statutory structure. Additionally, the Court held that a person’s freedom of speech and freedom of association was not

violated, as expression in the form of violence is not protected by the Charter. How the Supreme Court of Canada strikes the balance between rights and national security in the Harkat case will be instructive. It also will be interesting to see to what extent the broad definition of terrorism and the expanded procedures of the Anti-Terrorism Act will be used in dealing with the seventeen Ontario suspects arrested in June, 2006. The early indications are that the powers under the Anti-Terrorism Act were not used but police are already calling for the retention of these broad powers and even for extending them.

Racial Profiling

The breadth of the definition of terrorist activity does lead to problems with other statutes. For example, the Office of the Superintendent of Financial Institutions (OSFI) creates a "consolidated" list of entities suspected of engaging in or supporting terrorist activity. Financial institutions must freeze assets of any listed entities. This system allows for broad discretion and encourages discretionary application of the list by the financial institutions: it is not just the people on the list whose assets must be frozen but even other names that resemble those on the list. This has a disparate negative impact on Arab and Muslim communities, and "in short, race and religion, through the use of names, becomes a proxy for risk." It is this kind of application of apparently neutral laws that raise serious equality issues through racial profiling.

We do not need to look very far to find other examples of racial profiling, especially in the "flying while Arab" context. Maher Arar is the subject of a Canadian inquiry: an Iranian professor, Mr. Arar, spent a month in a Canadian jail for making a reference to his bag exploding if it was stuffed under his seat. Author Rohinton Mistry discontinued his book tour in the US because he was stopped at the border so often. Like Mistry's award winning novel, our approach to anti-terrorism needs "A Fine Balance."

At the Senate Committee Hearings in 2005 reviewing the Anti-Terrorism Act Canadian Muslim and Arab groups argued that if law enforcement agents were going to use profiling in their investigations, profiling should be based on behaviour, and not ethnicity or religion. However, in another Globe and Mail article, Conservative MP Kevin Sorenson cited a different opinion: "(y)ou don't send the anti-terrorist squad to investigate the Amish or the Lutheran ladies. You go where you think the risk is."

Unfortunately for Ahmad El Maati, law enforcement agents thought he posed a risk and that thinking led to his detention and torture in Syria over an Ottawa visitor's guide. In August, 2001, Mr. El Maati, a Kuwaiti-born Canadian truck driver, was making a delivery to the US. His usual truck was in a shop for repairs and his company assigned him a replacement truck. US customs pulled over Mr. El Maati for an inspection and found a

visitor's map of a government building complex in Ottawa. Mr. El Maati was not familiar with the Ottawa area; however, the last driver of the truck was based out of this city.

Mr. El Maati was held at the border for eight hours. US officials took his fingerprints, photographed him and took a retina scan. Later in 2001 he returned to Syria for his wedding. Syrian military intelligence arrested him and tortured him. In 2002 they sent him to Egypt. In one interrogation session he was asked to identify a copy of this same map that had held him up at the US Border earlier that year. When a close coworker of El Maati was interviewed for a news story, he said, "If I was a border person and I saw this map with a Middle Eastern-looking person and all these nuclear sites and all these government installations, I can understand why they said, 'Well, hey pal, what are you doing?'" Irwin Cotler's description of our times being one when fear tends to overcome rationality seems to apply not only to border officials but to friends as well.

The phenomenon of profiling Arabs and Muslims has even affected pop culture. Recently, hit Fox TV series "24," where some of the villains "happen" to be Muslim, ran a disclaimer before one of its shows, featuring Canadian star, Keifer Sutherland, teaching us that while terrorism is a critical challenge to America and the world, it is important to know that the American Muslim community denounces terrorism too. These ads ran in the US, but there was a call to air the same ads in Canada as well to avoid or counter the negative images here.

There are domestic examples as well, that don't require approaching borders, and the effects are damaging to minority communities. The Ontario Human Rights Commission published a report in 2004 documenting the effects of racial profiling on individuals and communities, and some of the costs including feelings of shame, powerlessness and fear of authority. In 2005 the Canadian Council on American-Islamic Relations released the results of a survey they completed that showed that significant numbers of young, Arab males had been visited by either the RCMP or CSIS since the terrorist attacks of 2001. "It's safe to say that the overall consequence has been one of alienation, loss of trust in our security agencies and civic cynicism," said the Council's executive director, Riad Saloojee. One wonders if this was a factor for the young suspects allegedly involved in the recent Ontario plots.

Racial Profiling offers a simple solution to complex problems and in the end only adds to the root causes of terrorism in the world. But is it realistic to say that profiling should not be used at all? Profiling of some kind can't be completely ignored in the current context, and there are strong arguments to say that law enforcement agents must use profiling as an enforcement tool; however, profiling must be restricted to relevant grounds. If profiling is to be used as a tool, it must be used with great caution because, notwithstanding the obvious utility of this tool, the dangers are extremely high. Some may say, in fact, that the dangers are too high. In the past, Canada denied profiling

even happened. Now we accept that it is done, but that it must be done carefully. Race or ethnicity cannot be used as a proxy for security risk in our efforts to combat terrorism. It seems that Canada has developed its own approach to profiling, and is becoming increasingly aware of the dangers of racial profiling. Hopefully this knowledge will survive the next terrorist threat. How Canadians respond to the June 2006 arrests in Ontario will provide interesting new insights. The situation may also provide the context for a test of Canada's Anti-Terrorism Act and a challenge to its constitutionality.

Privacy & Information Flow

Privacy and access to information may be one of the major casualties of the "war" on terror. In his article on terrorism, Irwin Cotler emphasizes the differences between Canada and the US on several fronts, but especially in respect to privacy and the free flow of information. He argues that in the US "secrecy" prevails while in Canada "access" is still the norm, and that Canada is much better than the US on the "secrecy" vs "access to information – transparency" front. This may be true, but there are still problems in Canada.

> Post " 9/11" amendments to the Canada Evidence Act included the power of the Attorney General to issue an Attorney General's certificate to keep information in a terrorism proceeding secret:
>
> 38.13(1) The Attorney General of Canada may personally issue a certificate that prohibits the disclosure of information in connection with a proceeding for the purpose of protecting information obtained in confidence from, or in relation to, a foreign entity as defined in subsection 2(1) of the Security of Information Act or for the purpose of protecting national defense or national security.

This certificate must be filed in Federal Court. When the Attorney General issues this certificate, then disclosure of information shall be prohibited in accordance with the terms of the certificate. The AG certificate expires after 15 years but may be reissued.

This AG certificate is different from the security certificates that have been featured so prominently in the media: the former keeps information secret whereas the latter concerns the detention and deportation of individuals. What is different about the Canadian response compared to that in the US is that we did not rely generally on detention in response to the September 11 attacks. As I will discuss in detail later, security certificates existed in Canada since 1991 under the Immigration and Refugee Protection Act. The key difference is that they have always included a procedure for judicial oversight.

Attorney General's certificates are one example of the Canadian Government's power to keep information secret in a very particular circumstance. Breaches of a Canadian

citizen's privacy may be happening without the citizen even knowing about it, including the disclosure of private information by private sector companies. When it comes to border crossings, Lisa Austin, a professor at the University of Toronto Law School, argues that it is not so much the specific searches and surveillance at the border that we need to worry about, but a new type of surveillance that is being developed as a result of information gathering by the private sector. Austin describes this new surveillance as "one that depends on collecting, storing, aggregating, sharing and linking vast amounts of information about people and then using this information for screening purposes." These fears have played out with US Government officials ordering large search engines such as Google to share some of the personal information of its clients as well as phone and internet companies providing information about students on university campuses.

Austin writes that this kind of surveillance shifts the focus from borders to non-border areas where the information is collected and intrudes on the privacy of people who might never be subject to border searches. For example, information that you might expect an airline to collect could be used by law enforcement agents in ways that you had not contemplated. This kind of information gathering is expressly mandated under Canada's Public Safety Act. Austin argues that these activities undermine privacy, and have few accountability mechanisms. Recently, the United States has proposed an alternative to passports at the Canada-US border in the form of biometric cards, called PASS cards. The cards are inexpensive and are purported to make border crossing more efficient. One wonders about what uses this personal information could be put to. There is also evidence that passengers are willing to subject themselves to iris scans if it means greater efficiency and speed of processing.

In October, 2004, the province of British Columbia amended its privacy legislation in response to a report released by the province's Information and Privacy Commissioner. This report considered the privacy implications that the USA Patriot Act would have in British Columbia. The Patriot Act was enacted quickly in response to the September 11 terrorist attacks and it amended and extended many US laws concerning intelligence and counter-intelligence activities, information sharing and terrorism.

The Commissioner heard from over 500 individuals and organizations on the issue, and there was a general consensus that the Act allowed (even required) a US located company to disclose records of Canadian subsidiaries to the US government. In many cases these subsidiaries had to choose between obeying Canadian or American privacy laws. The Commissioner found that in the absence of evidence of safeguards it was prudent to assume that "US authorities are unfettered" in their ability to seek an order for the disclosure of records. Similar problems exist in other provinces such as Nova Scotia, which has made a modest legislative response.

The report made several recommendations, including changes to British Columbia's privacy legislation, developing a provincial litigation policy, and audits of information sharing agreements. However, the report included less concrete recommendations as well: "provincial actions alone are not sufficient to address risks posed by transfers of personal information across national borders… (n)ational dialogue and action are required."

Here in the Maritimes, the Auditor General of Nova Scotia's annual report for 2005 included a chapter on electronic information security and privacy protection. The Auditor General noted that the Nova Scotia government used Canadian subsidiaries of US corporations for information management, including a company used to store backup tapes for the management of the government's mainframe computer system. The Auditor General's recommendation was for the Nova Scotian government to continue to monitor the implications of the USA Patriot Act as it relates to the privacy and security of personal information held by the government. However, one has to wonder if this is enough.

One of the key things that distinguish us from certain countries is that issues of privacy are discussed in a democratically elected state. If you think back, for instance, to the case summaries on employee privacy rights produced by the Privacy Commissioner then it becomes clear that not only can you make complaints, not only will your complaint be investigated, not only is the investigation public, but anyone can access the results of the investigation on the internet. And if you're unhappy with the way things are going you can make an issue of it at election time. There are still significant problems but the protection of privacy is advancing on some fronts.

In Canada, breaches of privacy are subject to checks and balances, even if sometimes the checks do not come along for another four years. And the situation in Canada isn't necessarily true in other "like-minded" countries; there are differences in attitudes toward both privacy and national security, even among democratically elected states. Our anti-terrorism legislation was subject to healthy debate in Canada while the USA Patriot Act was enacted without discussion, either within government or the general public. And there is nothing in Canada comparable to the Homeland Security Act or Department; pervasive violations of privacy rights as set forth in US legislation have no counterpart in Canada. And our legislation comes complete with its own re-evaluation mechanism: the sunset clause. The biggest challenge in the war on terror is for us to strike a balance between the need for security and maintaining freedoms. This challenge will be accentuated by the recent arrests of suspected terrorists in Ontario.

But maybe we do not have to worry exclusively about the courts' role in maintaining freedoms. Perhaps we can put our faith in the democratic arena: that oversight by media, the professional bar, civil liberties groups and civil society along with Parliament

are best equipped to guarantee civil liberties under the Anti-Terrorism Act. This is what Irwin Cotler argues: is public vigilance the best form of a “sunset clause”?

III. Technology and the State’s Right to Know

Advances in technology have made it much easier to violate privacy, and legal protections have not kept pace with technological advances. I have written before about the idea that technology could break down barriers and advance equality on many fronts, but technology is a double edged sword when it comes to rights. In a report prepared for the Canadian organization Rights and Democracy, Deborah Hurley points out that the political will to use technology to advance equality is lacking and technology is often put to more sinister purposes. Just like law, technology is not neutral and value free, although it is often argued that it is. Technology is embedded in a social context, and, when it comes to technology, context is everything.

While technology has the potential to promote equality among people by increasing access to information for all that has not been its major impact. Instead information has become a commodity to be marketed by the corporate world, and used by political forces as a powerful propaganda device. Not only has the advance of technology accentuated the economic divide between those who can afford access to the internet and those who cannot, the World Wide Web has been dominated by those who want to sell us things be they commercial products or a particular political ideology.

The internet has unfortunately become a powerful force for the promotion of hatred and intolerance. The use of the internet by people like Ernst Zundel to promote his message of anti-semitism and hatred is just one example. A more recent source of concern arises from the June 2006 arrest of suspected terrorist bombers in Ontario. It would appear that many of the alleged terrorists extreme Islamic views were inculcated by views expressed on websites. People no longer have to meet to conspire to commit violent acts; it can all happen online. The prevalence of these websites promoting hatred, extremism and violence, is a major challenge for law enforcement and legal regulation. Thus technology has become a major vehicle for the suppression of human rights and the promotion of hatred and intolerance. It is far from a force for equality.

One of the many alarming aspects of the recent arrests of suspected terrorists in Ontario is the targeting of youth to join the holy crusade against the West and its values (the jihad). While websites were one vehicle, the infiltration of mosques, schools and community centers are other ones. The success of this propaganda exercise is based in part on a sense of marginalization and victimization felt by some young people. They are vulnerable to the siren call of joining a noble and just cause. A recent Globe and Mail editorial raises the importance of the “ideology of victimhood” as fertile soil for terrorist activities.

In Canada, Muslims do not find themselves living in separate communities as in Britain, where in 17 primary schools, 90 per cent of students are Bangladeshi. They are not living in sprawling suburban ghettos, as in France. Female Muslims are not forbidden to wear the traditional head scarf in public schools, as in France. Schools make enormous accommodations—barring male lifeguards, for instance, to permit special swimming periods for Muslim girls.

And Canada is not in Afghanistan to oppress Muslims. Afghanistan under the Taliban was the most repressive and backward land on Earth. Canada is there to help that nation rebuild and to prevent it from becoming a leading base for international terrorism again.

But the ideology of victimhood is attractive to some young people because it explains everything, and the young person who takes up the cause has no more identity problems. The Canadian Council of Muslim Theologians praised police for taking action to protect Canadians, including Muslims, from alleged terrorist acts. That was a welcome statement. As Mr. Khan says of extremists, “We must not allow these people to shake our values that we have in Canada.”

In an interesting special on the “Enemy Within” the CBC Television National aired a special on June 6, 2006 on the retreat from multiculturalism in places like the United Kingdom and the Netherlands. There is a clear backlash against the separatism of Muslim communities in parts of Europe and their rejection and opposition to traditional Western values. Integration of different cultures, rather than a fuzzy multiculturalism, has become the rallying cry of many people concerned about terrorist activities and the threat of the enemy within. It will be interesting to see whether the arrest of terrorist suspects in Ontario will be a setback for multiculturalism, or merely a wake-up call for better education in the challenges of combining a diverse population with the promotion of core Canadian values.

Technology and the free flow of information will be vital to efforts to maintain a tolerant and multicultural Canada and also one that continues to respect its core values such as freedom and equality, expressed in the Charter and elsewhere. It is important to explore why some young Muslims in Canada are attracted to the extremist form of the “jihad” (holy war) and what needs to be done to offer alternative ways of expressing youthful protest. There needs to be a clear and effective message that promoting terror and violence is not a cool thing to do and the price for all concerned will be very high.

The relationship between technology and human rights is well illustrated by the example of technology used in 1989 at Tiananmen Square, China. A company from the United Kingdom had manufactured surveillance cameras for China and the World Bank had financed their installation, intended to monitor traffic flow and regulate congestion. The

cameras were later used to identify protesters at Tiananmen Square, and their images were broadcast over state television. Of course the manufacturers and the World Bank insisted that they had no idea that their technology would be used in this way; however, the World Bank later funded the same “traffic” surveillance system in Tibet in an area dedicated to pedestrian traffic.

We live in a surveillance society, no matter where we live. Currently the average person in the United Kingdom is caught on closed circuit television 300 times each day. Hurley writes that “the risk, if these technologies are deployed to take ever greater note of us, is that the fundamental principle that a person is presumed innocent until proved guilty, a human right and central tenet of our legal system, will be inverted, so that all of us will have become suspects.” This is one of the dangers if the pendulum swings too far to the side of protecting national security.

Genetic and Psychological Testing

Technology can also be examined in the context of genetic testing. In the world of Crime Scene Investigation (CSI) television shows, the importance and value of DNA is clear. A DNA databank of genetic samples taken from convicted offenders can be used for the “neutral” purposes of solving crimes. The problem is that the DNA in the bank could also be available to determine a “crime gene” and could result in certain people being segregated, mistreated, or prevented from having children. To quote academic Janet Hoeffel:

Imagining then that not only law enforcement officials, but insurance companies, employers, schools, adoption agencies, and many other organizations could gain access to those files on a ‘need to know’ basis or on a showing that access is ‘in the public interest’. Imagine then that an individual could be turned down for jobs, insurance, adoption, health care and other social services and benefits on the basis of information contained in her DNA profile, such as genetic disease, heritage, or someone else’s subjective idea of genetic ‘flaw’.

Psychological testing in education and the workplace is another area that blurs the privacy lines when it comes to the state’s right to know. In the employment context there is a view that testing cannot be an invasion of privacy because the employee, or future employee, is giving his or her consent to be tested. But are these searches of the mind really consensual in this context? Refusal to take a test has serious enough economic consequences that it isn’t really an option, and consent, in this case, is nothing but forced.

Another form of employment testing that is becoming increasingly prevalent is integrity testing. These tests are designed to identify individuals with a high propensity to steal while on the job, or engage in other counterproductive work behaviours like tardiness,

sick leave abuse and absenteeism. In the past I have argued that it is easy to see how these tests could have a negative impact on particular cultural groups. For example, in some Aboriginal societies there is a more communal view of the ownership and use of property, which could lead to a different view as to what constitutes theft. A person may think that it was appropriate to use a pen from another person's desk that was not being used at the time, but this could be considered theft when presented as a hypothetical integrity test question. While there is little research information gathered on this topic there is no doubt that many other aspects of these tests are based on cultural assumptions.

The Criminal Context

The case of R. v. Stillman illustrates how complicated it can be to determine a reasonable expectation of privacy, a right I referred to earlier. There is also the difficult issue of the state's right to know. The accused in this case had been arrested and his lawyers informed the police that he would not consent to providing any bodily samples. Despite this, the police, under threat of force, pulled hair samples off the accused and took plasticine moulds of his teeth. A police officer then interrogated him for an hour, during which time the accused sobbed. He then went to the washroom where he used a tissue to blow his nose. The police seized the tissue from the waste basket and used it for genetic testing.

The Court found that both sections 7 (life, liberty and security of person) and 8 (the right to be secure from unreasonable search and seizure) of the Charter were violated in the seizure of hair samples, swabs and dental impressions. The use of the discarded Kleenex was also held to be a section 8 violation; however, the Kleenex was admitted as evidence under section 24(2) of the Charter, that states that evidence should only be excluded if it is established that the admission of it would bring the administration of justice into disrepute. So despite the fact that the accused had nowhere else to put the tissue other than in the waste basket, admitting it would not bring the system of criminal justice into disrepute.

There are many issues to discuss in this area: the reasonable expectation of privacy; consent; how the information was collected; how the data will be used; and how it will be stored. Again, from these examples, we see a picture of Canada where Canadians are generally very tolerant of violations of their privacy. We assume that the government is benign, that our privacy rights are not abused by the government, and that others are the targets. Much education is needed in this area in Canada. Later I will explore technology in the security context, and what considerations there are when we export technology to other countries.

The benefits of the surveillance society are easily articulated in the post “9/11” world that is focused on the need for security and constant vigilance against the forces of terrorism. It was on the basis of two years of close surveillance by the police and security officials that the arrest of suspected terrorists in Ontario was orchestrated. The value of pre-empting a plot that involved the storming of Parliament and the CBC, the be-heading of the Prime Minister and the kidnapping of other politicians, is undeniable. Surveillance and controlled invasions of privacy are crucial to the prevention of terrorist attacks. Whether the existing Criminal Code powers are adequate or whether the additional powers granted by the Anti-Terrorism Act are needed, remain to be decided. What is clear is that most Canadians are willing to sacrifice a high degree of privacy in the name of national security and the prevention of terrorism. The cases that are likely to emerge out of the 2006 Ontario arrests are likely to clarify how the courts will strike the balance between national security and privacy. Other important values, such as, the presumption of innocence and the right to a fair trial will also be tested.

There is no doubt that the state has a growing need to know and that technology makes this possible. The question is how far we should go in sacrificing privacy and the right to be let alone. Even in these unstable times, maintaining some zone of privacy is important to the Canadian way of life. Technology will not provide the limits on surveillance, but rather these limits will come from the laws enacted by our elected legislators and interpreted by our courts. It is vital that privacy and other core democratic values not be completely sacrificed on the altar of national security. To do so would be to let the terrorists win in a different way.

IV. Domestic National Security and Comparative Responses to the Terrorist Threat

Secure Borders

In this present day global village it has become increasingly easy to physically cross borders. However, technology and terrorism have made crossing borders a more complicated affair. Vancouver International Airport recently introduced iris scanners to fast track US-bound fliers, on a voluntary basis. According to the Airport these scanners make life easier for frequent travelers and allow border officials to “concentrate on catching criminals.” While this frequent flyer program is voluntary, it seems that there is great potential for privacy violations. If airports start with voluntary iris scanning, it is logical that voice scans, finger prints and smart cards are not far down the road. This is a view expressed by Stockwell Day the Minister in charge of security issues. Should privacy be sacrificed for the sake of efficiency? Consider Professor Austin’s examples of how this information could be used in ways you had never contemplated.

In 2002 Canadian, Maher Arar, was detained by US border officials and deported to his birth country of Syria. Arar was a casualty of human rights in the context of terrorism as he was sent to Syria to face torture. “Diplomatic assurances” do not guarantee against inhumane treatment. Likewise, Canada should not send prisoners to the US and deport people there if America does not obey international laws, such as, the Geneva Convention. Currently, prisoners in Guantanamo Bay are declared unlawful combatants who are not protected by the Geneva Conventions.

Former Deputy Prime Minster, John Manley, has called for an integrated North American security perimeter. He did this in his capacity as chair of the Canadian Council of Chief Executives Committee. Forcing Canadian and US citizens to carry biometric security cards will only heighten civil liberties activists’ fears about privacy violations. It is interesting to note that John Manley works for biometric firms who partly sponsor technologies like iris scans. He is also Chair of the Canadian Council of Chief Executives Committee which supported the study.

At the domestic level the response to terrorism has also raised serious issues for Canada. Once again this issue is addressed in a thoughtful Rights and Democracy publication. Iris Almeida and Marc Porret in Canadian Democracy at a Crossroads: The Need for Coherence and Accountability in Counter Terrorism Policy and Practice, make recommendations for improving the balance between national security and human rights by addressing issues such as, racial profiling, security certificates and growing invasions of privacy. The issue of security certificates under the Immigration and Refugee Protection Act has been in the news, as these allow people to be held for long periods of time with no charge being laid. Reasonable suspicion of a threat to security is all that is needed. In the case of Ernst Zundel, security certificates resulted in his ultimate deportation to Germany. This issue of security certificates is presently going before the Canadian Supreme Court, in the Harkat case and the nature of these certificates will be discussed shortly.

The response to terrorism also raises thorny issues of Canada’s relations with its powerful neighbour – the United States. Lloyd Axworthy in Navigating a New World: Canada’s Global Future discusses this issue in Chapter 4 under the clever title “How to Make Love to a Porcupine.” In addition to the usual challenges, such as NAFTA, the events of “9/11” have heightened concerns about border security and the need for an integrated border security strategy. The study referred to earlier by former federal Cabinet Minister, John Manley, calls for more continental integration of border security and sharing of information between Canada and the United States, that involves many limitations on the privacy rights of Canadians.

Lloyd Axworthy in his book sounds a cautionary note about too much integration of Canadian and American security and raises the spectre of the Homeland Security Act as “big brother.”

The opaque nature of the co-operation is a worry. Take for example the extensive surveillance system authorized under the Homeland Security Act. This is a plan to establish a data pool on a broad sweep of individuals by mining various sources, such as credit card accounts, bank accounts and other confidential files – a version of Orwellian spying that is about to come true.

Former federal Cabinet Minister Axworthy is also wary of the Americans’ willingness to trade away basic values in the name of security.

Politicians and bureaucrats in Washington, as this case demonstrates, have little regard for what we consider our fundamental values, especially when security is at stake. In the absence of clear rules, muscle prevails and serious damage can be done to our interest. We need to define our own strategy for managing those interests and not just be in a reactive mode. The place to start is by defining the border security issue in the mode of a community, not a fortress.

I support the views expressed by now President of the University of Winnipeg, Lloyd Axworthy. Of course, we must co-operate with our powerful neighbour to the south on security as well as many other matters of mutual interest. However, Canada should have a significant say in this form of co-operation and it must not sacrifice its national autonomy or core Canadian values by elevating national security above all other rights and values. The traditional Canadian values of moderation and balance still serve us well.

Security Certificates

A Security Certificate is a way for the government of Canada to remove permanent residents or foreign nationals who are deemed to pose a security risk. It can be used in a pre-emptive fashion. As I mentioned earlier, they are not a result of the September 11th attacks; security certificates have existed since 1991 in the Immigration and Refugee Protection Act. Certificates must be issued by the Minister of Citizenship and Immigration, as well as the Minister of Public Safety and Emergency Preparedness. They cannot be issued under the Anti-Terrorism Act as this Act is primarily about investigation and prosecution; however there are certificates under this act that allow certain evidence to be kept secret, and the Attorney General can issue these specific certificates under 38.13 of the Canada Evidence Act, as I discussed earlier.

For a Security Certificate to be issued, a Judge of the Federal Court must determine whether or not the certificate is reasonable. The standard of proof is very low; the Judge

must determine whether or not the certificate is “reasonable,” as opposed to either the civil standard, which is the “balance of probabilities,” or the criminal standard, which is “beyond a reasonable doubt.” It is hard to believe that the standard for deporting someone from the country or of holding them without charges is only “reasonableness.”

A summary must be provided and the person named can respond. Neither the detainee nor his or her lawyer have full access to the evidence against him/her, as much of it is kept under a veil of secrecy in the name of national security. If the Judge finds that the Security Certificate is reasonable then the Certificate automatically becomes a removal order. It cannot be appealed. When the question of reasonableness is posed to the Court, it generally takes a long time before a decision is made. In the interim the person named in the certificate is usually held in detention, and often is placed in solitary confinement.

In the winter of 2005 the Federal Court held that one such Security Certificates signed by the Minister of Citizenship and Immigration and the Solicitor General was reasonable. The Ministers argued that a man named Ernst Zundel was a security threat due to his ties to the White Supremacist movement. The Certificate was signed on the basis that Zundel was a threat to Canada on security grounds, but Zundel had lived in Canada since 1958. Zundel argued that he never committed a crime, nor was he involved in acts of violence or other illegal activities.

Unfortunately for Zundel, Justice Blais followed the previous case law in which “danger to security” was given a large and liberal interpretation. Blais stated that:

White Supremacists are defined as racists, neo-Nazis and anti-Semites who use violence to achieve their political objectives. Leading White Supremacists may inspire others to use or threaten use of violence. Mr. Zundel is viewed by White Supremacists as a leader of international significance and was viewed as the patriarch of the Movement for decades.

Regarding the secrecy of the evidence, Blais wrote:

> As I mentioned publicly during the hearing, I understand Mr. Zundel’s frustration regarding his inability to access the classified information; nevertheless, I carefully reviewed the classified material and decided that it was not possible to provide more information than was provided in the Summary, as the classified information would be injurious to national security and to the safety of persons if disclosed.

One of the prices of a growing emphasis on security is an increasing lack of access to information, even when people face serious consequences such as criminal conviction, or, in the case of Mr. Zundel, deportation to stand trial elsewhere. There was an

admittedly weak link between Zundel and violent organizations; regardless, the Court found that the Security Certificate was reasonable, and the Certificate became a removal order. Mr. Zundel was deported to Germany, where he is now on trial. While Ernst Zundel is no champion of human rights, his basic rights also deserve to be protected.

Canada, United Kingdom (UK) and United States (US) Responses

Let me now turn to responses to the terrorist threat in the United Kingdom, US and here at home. The Anti-Terrorism, Crime and Security Act was enacted by the UK Parliament in 2001. Under this statute, the Home Secretary can issue a certificate against a non-UK national if he or she reasonably believes that the person's presence in the UK is a risk to national security and he or she suspects that the person is a terrorist. This decision can be reviewed for reasonableness of belief and suspicion by an independent tribunal.

In a case called A(FC) v. Secretary of State for the Home Department the House of Lords found that the Act, in permitting the Secretary to detain on mere suspicion, was inconsistent with the UK's Human Rights Act. Further, the detention of foreign nationals was found to be discriminatory in that there was no justification for distinguishing between UK and foreign nationals.

In response, the UK Parliament enacted the Prevention of Terrorism Act which gives control to the courts to supervise the making of orders. The Foreign Secretary must apply for permission to make an order and the Court must be satisfied that the order is necessary to protect members of the public from the risk of terrorism. While at first glance it seems that the new Act has greatly increased the checks on violations of a person's liberty and security of the person, the hearings can be held without the presence of the person in question and even without notice to that person. It should always be cause for concern when a person is not entitled to a full answer and defence or, in other words, a fair trial.

Prime Minister, Tony Blair's efforts to fight terrorism at home received a second blow in March 2006 as reflected in the following news summary, entitled "British Lords again reject changes to Terrorism Bill":

> Britain's House of Lords rejected yesterday for a second time a proposal from Prime Minister Tony Blair's government to make glorification of terrorism a crime. Many peers felt the Terrorism Bill, drafted in the wake of the July 7 bombings in London last year, is too vague and would curb freedom of speech. The outcome means the bill returns to the House of Commons for more debate.

In April 2006, in his judgment in the case of Re MB, Mr. Justice Sullivan issued a declaration under section 4 of the Human Rights Act 1998 that section 3 of the Prevention of Terrorism Act 2005 was incompatible with the right to fair proceedings under article 6 of the European Convention on Human Rights. Mr. Justice Sullivan held:

> To say that the Act does not give the respondent in this case, against whom a non-derogating control order has been made by the Secretary of State, a fair hearing in the determination of his rights under Article 8 of the Convention would be an understatement. The court would be failing in its duty under the 1998 Act, a duty imposed upon the court by Parliament, if it did not say, loud and clear, that the procedure under the Act whereby the court merely reviews the lawfulness of the Secretary of State's decision to make the order upon the basis of the material available to him at that earlier stage are conspicuously unfair. The thin veneer of legality which is sought to be applied by section 3 of the Act cannot disguise the reality. That controlees' rights under the Convention are being determined not by an independent court in compliance with Article 6.1, but by executive decision-making, untrammeled by any prospect of effective judicial supervision.

In the United States, the 2001 terrorist attacks prompted the passing of the Authorization for Use of Military Force Resolution which included authorization for the President to use "all necessary and appropriate force" against "nations, organizations, or persons" associated with the September 11 attacks. A US citizen, Yaser Esam Hamdi, was captured during military operations in Afghanistan and detained without charges or a trial for three years, on the basis that he was an "enemy combatant." In Hamdi v. Rumsfeld the US Supreme Court found that Hamdi had to have a hearing before a neutral decision maker to contest the basis for his detention.

There have also been recent revelations that President Bush and his agents were intercepting emails of Americans on a much wider scale. This has allegedly been happening over a long period of time. Both the UK and US Courts have found that arbitrary and unreviewable detention and arrest are unacceptable as a means to combat terrorism. It will be interesting to see how Canada views this matter in light of the June, 2006 arrest of terrorist suspects in Ontario. The Canadian Supreme Court will have the benefit of the precedents in both the United States and the United Kingdom.

Canadian responses to the terrorist threat have been challenged in court as well. One such challenge was to the new investigative hearings under the Criminal Code. This occurred in the context of the high profile Air India tragedy, where the accused were ultimately acquitted. Air India was Canada's major terrorist trial to date and the matter will now go before a commission of inquiry headed by retired Supreme court Justice, John Major. The Supreme Court of Canada found that "although terrorism changes the context in which the rule of law must operate, it does not call for the abdication of law."

The investigative hearings were found to be constitutionally valid because the hearings were simply investigative and therefore not self-incriminating. If necessary, the Court could extend immunity for compelled testimony at these hearings. More recently, the definition of “criminal organization” was challenged in a British Columbia Supreme Court in the context of a motorcycle gang. The Court held that the definition was too vague and therefore of no force and effect. This reasoning could also be applied to aspects of the Anti-Terrorism Act especially its broad definition of terrorism. New court challenges will likely emerge for the recent Ontario arrests of suspected terrorists.

Shortly after the arrest of seventeen terrorist suspects in Ontario, the Federal Court of Canada ruled that even in times of terror, fairness and the rule of law must prevail. Many would view Mr. Khadr as one of Canada’s original home grown terrorists, and he is clearly a member of a family that has been linked to terrorist activities. The twenty three year old Abdurahman Khadr was captured n Afghanistan and for months was held as an “enemy combatant” by the United States forces in Guantanamo Bay, Cuba. However, he has never been charged with a crime. He is considered the most moderate member of a family of notorious extremists, some of whom have been linked to Al-Qaeda. This young member of the family has denounced terrorism and even risked his life as a spy for American intelligence. Having won his right to a passport he praises the Canadian justice system and vows to be a model citizen.

While his case raises eyebrows in light of the June, 2006 arrest of terrorist suspects, it is also a triumph for the presumption of innocence and hailed by some as a victory for the rule of law in Canada. In the absence of evidence to indicate that Mr. Khadr should not receive a passport and proof that he poses a genuine security threat, I agree with the courts vindication of his rights. Passports should not be denied on the basis of suspicions that cannot be verified or supported nor should there be guilt by association or family status.

V. International Relations and National Security

I will now turn to the intersection between national security and international human rights. Arar is not the only casualty of the clash between security and human rights. The 2001 terrorist attacks happened in the United States, and Canada shares a border with the US. But we are seeing that other countries are using US rhetoric and policies to justify their actions; they are, in effect, co-opting the war on terror. You can see the same language of anti-terrorism being used by the governments of Russia, Liberia, Zimbabwe, and China: countries with questionable human rights records. The rhetoric is justifying state terrorism.

How is Canada implicated in the human rights of other countries? We need to consider the impact of international trade and human rights for the answer. An illustrative

example is that of the Golden Shield project in China. The Canadian organization Rights and Democracy describes the Golden Shield Project as “a gigantic online database with an all-encompassing surveillance network – incorporating speech and face recognition, closed-circuit television, smart cards, credit records, and internet surveillance technologies.” Canada, with the assistance of Nortel, is supplying Canadian technology for China’s Golden Shield project. This underscores the importance of ensuring that human rights are on the agenda as Canada seeks to expand its trade relations with China, the awakening giant on the international scene. The links between trade and human rights are vital as explored by a 2003 Rights and Democracy Think Tank held in Ottawa.

China poses a real dilemma for countries, such as Canada, who have concerns about China’s poor human rights record but a strong desire to tap the lucrative Chinese market. The double edged nature of technology is clearly demonstrated in China. It is vital to China’s growing economy and link to the West, but it also gives the Chinese Government a major tool for surveillance and suppression. Within China, access to the internet is strictly regulated, and the price of violating these laws can be death. There is a very high degree of internet censorship in China and it has limited the extent to which the internet can advance the cause of freedom of expression, especially if that expression is in the form of dissent.

The double edged nature of technology and increased access to the internet is clearly demonstrated by the situation in China. A growing access to the internet makes it more difficult for the Chinese Government to control the flow of information, even with severe legal sanctions for “inappropriate” use of the internet. Even in China these laws are difficult to enforce. On some estimates there are thirty million bloggers in China some of whom expose Government corruption or wrong doing and bring to light issues such as mining accidents that in the past state authorities have been able to hide. There is emerging a “virtual” Chinese civil society that can engage in dialogue and criticism of the state in ways that are difficult to control. In this sense the internet has been a force for free speech and a more democratic China. However, the story does not end there.

As mentioned above, the internet also provides a powerful tool for surveillance and the more effective repression of dissent and freedom of speech. Not only can the Chinese Government monitor the internet and try to hold users strictly accountable for any “abuses,” it can also enlist private companies in this process of censorship and control. This was demonstrated when the search engine, Yahoo, provided information about people using its Chinese internet services, that led to the arrest and detention of some people expressing dissident views. More recently the search engine, Google, has made a deal with the Chinese Government, whereby certain websites will be off limits to users in China. Thus Google is co-operating with the Chinese authorities in a pre-emptive campaign of censorship. The co-option of private sector companies (in search of

business and profits), to assist the state in spying on its citizens is a serious and growing threat to privacy.

In spite of these problems, Louise Arbour, the United Nations High Commissioner for Human Rights and former Justice of the Supreme Court of Canada remains optimistic about the prospects for better protection of human rights in China. This is a view that is not readily shared by activists, who are regular targets of police surveillance. There are certainly many human rights challenges in China and Asia more generally, but it is vital to work with China and other Asian countries rather than writing them off as hopeless. This is a vital part of High Commissioner Arbour's message. I expect these human rights challenges to be a major topic at the International Center for Human Rights and Democratic Development's (Rights and Democracy's) June 14 and 15, 2006 Think Tank on Asia, being held in Toronto, Ontario. Human rights must remain on the agenda as we explore greater trade relations with Asia and other parts of the world facing repression of human rights.

Returning to the importance of technology as a force for both good and evil, the case of China is instructive. Canada must pay attention to how the technology it exports will actually be used. A common response of technology companies is that technology is neutral. But if we think back to the traffic cameras at Tianenmen Square we can see that the context of technology must be considered. Once again I stress that technology is not neutral and value free. Technology is embedded in a social context, and, when it comes to technology, context is everything.

The Canadian Advanced Technology Alliance (CATA) states on its website that it is focused on ensuring the protection of privacy and integrity of personal data. But how will it do this if it is involved in selling technology to China? This clearly is not neutral technology. One example of Golden Shield technology is "smart cards," cards with all of your personal information on them. Smart Cards are like identity cards, but they can be scanned from a distance without you knowing. This means that the Chinese government could have immediate access to records on every citizen in China, and this is all dependent on Western, or Canadian, technology. Similarly, the "Great Firewall of China" has been built; Chinese citizens don't have free access to the internet. Citizens face the possibility of the death penalty for using the internet. When we sell our "neutral" Canadian technology to countries like China, we are implicated in their human rights abuses. But instead of Canada taking a stand and refusing to trade with these countries, or putting conditions on trade, the dollar has too often prevailed over human rights. The export of technology as with the export of nuclear reactors, should be accompanied by restrictions on its use and mechanisms of accountability.

It would be unfair to single out China as the only country that uses technology to repress dissent. This is a widespread phenomenon, especially in the context of the war

on terrorism. As mentioned earlier the rhetoric of anti-terrorism has been co-opted for purposes of state suppression. Since the events of September 11, 2001 there have been significant shifts in the nature and conduct of international relations. In many respects both the language and practices of international diplomacy have changed.

In recent years, we have been witnesses to a dramatically changing world in which our old concepts of international peace and security, human rights and democracy have been challenged by the perverse logic of terrorism and the inflammatory rhetoric and discourse of anti-terrorism. The devastating atrocities of “9/11” and the global reaction to them have raised many new issues for human rights defenders and advocates of democracy alike. The use of terror and the negation of dialogue in a world which depends on peace and human development both deserve attention and need to be addressed.

Although we now realize that the world is not as safe as we had once believed, we must not allow fear, suspicion, prejudice and military might to be the defining features of international relations. Rather, we must redouble our efforts to create optimal conditions for international peace and security; namely, respect for human rights, democracy, justice, the rule of law and dialogue.

There are a growing number of reports which show that even in countries with strong democratic traditions, important civil liberties, human rights and democratic values are under siege. Clearly, the balancing of individual rights against the security interests of the state has in practice tended to tip in favor of the state. International human rights norms that had been deemed beyond question prior to September 11, 2001 have suddenly become open for reconsideration.

There are many examples of this erosion of civil liberties since September 11, 2001. Some states have passed legislation restricting freedom of expression and freedom of the media. The public’s right to know has been curbed in several states and in some cases, the inviolability of journalists’ sources has been placed at risk. Other states have used the so-called international “war on terrorism” as a pretext to further crackdown on, target and repress political dissidents, separatists and religious groups.

There are many causes for concern but all is not bleak. There is a growing awareness of the need for all countries in the world to be concerned about human rights violations, wherever they may occur. There are advantages to the global village as the world is watching when it comes to abuses of human rights in once-isolated parts of the world. There has also been some overdue attention to the root causes of violence and terrorism in the world. Unfortunately, most of this attention has been in the form of words rather than actions. The Millenium Development Goals are a case in point.

VI. Economic Disparity and the Millennium Development Goals: Reducing World Tensions

In addition to the other kinds of discrimination that are at the roots of violence and instability in the world, the great disparity in wealth between different parts of the world is a major problem. Many other forms of discrimination also have elements of socioeconomic discrimination as well. This economic disparity between the West and the developing world is the garden from which terrorism has grown. It is not the only cause but it is an important one. With this in mind, an attack on poverty is the primary Millennium Development Goal.

There are eight Millennium Development Goals adopted by many countries and sanctioned by the United Nations in 2000. Time and space do not allow me to do more than list the goals but they are a vital part of the world's strategy for peace and progress. These goals are to:

1. Eradicate Extreme Poverty and Hunger;
2. Achieve Universal Primary Education;
3. Promote Gender Equality and Empower Women;
4. Reduce Infant Mortality;
5. Improve Maternal Health;
6. Combat HIV/AIDS, Malaria and other Diseases;
7. Ensure Environmental Sustainability; and
8. Develop a Global Partnership for Development.

As Rights and Democracy explored in their June 2005 Conference Report – Implementing the Millennium Development Goals: Our Human Rights Obligation, there is a clear link between these goals and human rights. In September 2005 there was an important United Nations Summit in New York to assess the progress being made in achieving these ambitious goals. At these same meetings attended by the largest number of world leaders in history, there was also consideration of the reform of key United Nations institutions—including the United Nations Commission on Human Rights. Canada was a voice for human rights and the need to reduce the disparities between the haves and have-nots. However, its own contributions to the developing world are well below the international target. The slow pace of institutional change is disappointing, as has been the real progress on reducing poverty in the world.

Canada also has an important role in establishing a model for matters of international trade by linking such trade to human rights as practiced by the trading partners such as China. International trade has an important place in an interdependent world. However, there are serious questions that must be raised regarding trade promotion and globalization. Global economic activity should advance the common good and

strengthen, not undermine local communities and families. Major trade negotiations should include broad-based citizen participation, and agreements should be ratified through genuinely democratic processes. Trade agreements should enhance the position of ordinary working people and the most vulnerable members of society, including women and people struggling to overcome poverty. They should protect and preserve the natural environment. Far from opposing trade agreements, we should ensure in a constructive dialogue that the rules created to govern international trade and investment reduce poverty, protect the integrity of the environment, and promote authentic human development and dignity throughout the world.

To achieve these goals, the framework that governments establish for international trade and investment activities should be accountable to the people in our own country and the countries with which we trade. A thorough public debate is imperative. Such a debate is also very timely as Canada and China are exploring the issue of linking trade with human rights. To really promote a more peaceful and stable world, Canada must take a leadership role in attacking the root causes of violence and instability. These include the many forms of discrimination and in particular poverty. To address these root causes of international turmoil is an investment in human rights that will pay rich dividends in a more peaceful world, where disagreements can be resolved by civil discourse rather than war, violence and terror. We owe this investment in human rights to future generations, even if the path ahead is unclear. To again quote from Lloyd Axworthy's book: "Traveller, There Is No Path. Paths Are Made By Walking."

It is noteworthy that the above quote refers to walking and not discussion about walking. A true investment in human rights requires actions as well as words. The words in the form of civil discourse can provide a good platform for action, but action there must be, before change can occur. This is true at all levels, but the implementation of the Millennium Development Goals would be an excellent step down the path to a more stable and peaceful world.

VII. Concluding Thoughts

At both the domestic and international levels we live in rather troubled times and the on-going threats of terrorism have moved concerns about national security to the top of the political agenda. The issue explored in this paper is what this means for human rights both in Canada and the larger world. In particular, I have focused on the need to balance privacy and national security but there are many basic human rights that have been subordinated to the promotion of national security. It has been difficult to examine rights to privacy without a broader consideration of related human rights. The access to information is a vital question in security measures but so are issues, such as racial profiling and liberty. Our human rights form on intricate web of which privacy is a part.

To draw upon an old slogan, human rights are everyone's business and that is just as true in the global village as in our smaller communities close to home. We are all diminished when we accept or ignore global human rights violations. It is vital that human rights be mainstreamed at both the national and international levels. Considerations of human rights must be integrated into matters of trade and security and not be regarded as an afterthought or hindrance to be overcome. Human rights should be kept high on the agenda at all levels of political discourse.

There is no question about the need for Canada as well as other countries to have a strategy to combat and ideally prevent terrorism both at home and abroad. However, this strategy must be carefully thought through and balanced in its approach to privacy and other human rights matters. Basic rights should not be quickly sacrificed on the altar of security. Iris Almeida and Mark Porret in their study done for the International Center for Human Rights and Democratic Development emphasize the twin pillars of "coherence" and "accountability" and these are good standards by which to assess Canada's anti-terrorism strategy. Former Justice Minister, Irwin Cotler, also emphasizes the importance of accountability and oversight mechanisms at the legislative, executive and judicial levels, a point that I have also emphasized in my presentations to the Senate committees dealing with the Anti-Terrorism Act. We should also not lose sight of the international norms for human rights as set out in documents, such as the Universal Declaration of Human Rights and our own Charter of Rights and Freedoms.

It can be argued that human rights are the allies and not the enemies of security at both the national and international levels. Good human rights protection and practices accompanied by the rule of law are vital to a stable national and international order. Integrating human rights into discussions of trade and international monetary policy is also crucial to the promotion of socioeconomic rights and a serious response to world poverty. Political instability and poverty provide the soil from which terrorist roots can sprout. Democratic states, practicing the rule of law and protecting human rights, are the best antidote to terrorism.

It should also be remembered that there is no clear constitutional right to national security in the traditional sense. National security is an important limitation on rights that can best be justified under section 1 of the Charter, when it manifests itself in the form of restricting basic rights, such as, privacy. There are clear links between national security and security of the person as guaranteed in section 7 of the Charter but section 7 is also linked to other important rights, such as privacy. It is vital to ensure that the governments advancing anti-terrorist strategies that limit our basic rights can justify these restrictions. In many cases the governments will be able to do so, but the burden is theirs. It is also vital to maintain an open, respectful and civil discourse about how to balance human rights and national security in a Global Village struggling with terrorism. The war against terror should also be waged in a non-discriminatory manner and the

temptation to lump people together or engage in unjustified profiling of groups, should be resisted. Human rights are ultimately allies in this struggle, and not enemies of national security.