Submission on the Three Year Review of the *Anti-terrorism Act*

CANADIAN BAR ASSOCIATION

May 2005

TABLE OF CONTENTS

Submission on the Three Year Review of the *Anti-terrorism Act*

PREFACE

The Canadian Bar Association is a national association representing 34,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the Anti-terrorism Review Group of the Canadian Bar Association, led by the Legislation and Law Reform Committee, and including members of the National Charities and Not-for-Profit Law, Citizenship and Immigration Law, Constitutional and Human Rights Law, Criminal Justice, International Law, and Privacy Law Sections and the Standing Committee on Equity, with assistance from the Legislation and Law Reform Directorate at the National Office. The submission has been reviewed by the Legislation and Law Reform Committee and approved as a public statement of the Canadian Bar Association.

EXECUTIVE SUMMARY

The Canadian Bar Association (CBA) appreciates the opportunity to contribute to the evaluation of the operation of Canada's anti-terrorism legislation. We expressed considerable concerns when the *Anti-terrorism Act* was introduced, though we understood the urge to respond to the tragedy that had just happened in the United States. In 2001, we advocated review and repeal of any hastily enacted legislation as soon as legitimate security reasons were no longer demonstrable, and we stressed the need for independent oversight of all extraordinary powers granted to law enforcement agencies. Since September 11, 2001, the federal government has enacted or proposed other measures, which dramatically expand state powers at the expense of due process and individual rights and freedoms.[1] Invasions on privacy and fundamental rights are creeping into Canadian law.

Scope of the Parliamentary Review

In our view, the three-year review should go beyond the *Anti-terrorism Act*, and look at the overall impact of all expressed anti-terrorism measures, as well as measures which operate in that context.

---

1 Examples include:

Criminal Code amendments to combat organized crime (Bill C-24) exempt police officers and police agents from liability for criminal acts.

The *Immigration and Refugee Protection Act* (IRPA) reduces rights of immigrants and refugees and diminishes fair processes to protect those rights.

Customs Act amendments (Bill S-23) permit customs officials to open mail over a certain weight, whether it is entering or leaving Canada.

The Smart Border Declaration and Action Plan between Canada and the U.S. institutes data collection (through systems such as PAXIS), information sharing, integration of databases, advance air passenger processing and joint risk assessment, In its April 2004 National Security Policy, *Securing an Open Society: Canada's National Security Policy*, the government indicated it would implement facial recognition biometric technology on the Canadian passport as part of the Passport Security Strategy.

The *Public Safety Act* 2002 requires airlines to provide passenger information to law enforcement agencies, which could be cross-referenced for law enforcement purposes completely unrelated to terrorism.

The Safe Third Country agreement turns refugee claimants away at the border without a hearing.

"Lawful access" proposals likely to be introduced in the near future will propose numerous techniques for conscripting private entities to take part in surveillance activities, possibly without meaningful oversight.

In determining the need for anti-terrorism legislation, this review should consider:

- appropriate objectives for an anti-terrorism strategy, including the distinction between national security and enforcement of criminal law;
- tools required for an effective anti-terrorism strategy;
- risks associated with terrorism and objective ways to evaluate suggested risks;
- the legal, constitutional and moral standards to be protected;
- a unified, national, independent review mechanism to ensure accountability of all agencies responsible for the advancement of anti-terrorism strategies, including law enforcement and intelligence gathering.

Rule of Law and Charter of Rights

Recognizing the rule of law as an overarching principle, the *Charter* rights and freedoms of particular importance to this review are:

- freedom of thought, belief, opinion, expression, conscience, religion, peaceful assembly and association (section 2)
- security of the person, including privacy (section 7)
- equal protection and benefit of the law without discrimination (section 15)
- security against unreasonable search or seizure and arbitrary detention (section 8)
- right to a fair trial and the presumption of innocence (section 11).

Defining Terrorism

Effective anti-terrorism legislation must identify with some precision what will be considered "terrorist activity". In our view, the definition in *Anti-terrorism Act* is too wide and too vague. The CBA recommends that terrorist activities be defined consistently in all Canadian laws relating to terrorism, adopting the definition in the UN *Convention for the Suppression of the Financing of Terrorism:*

> Any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

We also recommend that the *Criminal Code* be amended to require criminal intent for any terrorist offence. The CBA recommends that lawyers providing legal services to those accused of terrorist offences be excluded from the ambit of section 83.18, dealing with participation in or contribution to an activity of a terrorist group by directly or indirectly providing a skill or expertise for the benefit of a terrorist group.

Law Enforcement and Intelligence Gathering Tools

Canadian democracy rests in part on effective law enforcement and intelligence gathering. Terrorist activity has the potential to destabilize or destroy the very institutions and values that define our democracy. While individual rights and freedoms depend to some extent upon stable and democratic government institutions and the rule of law, the objectives of the government may, at times, be antithetical to those rights and freedoms.

An effective police force is essential to maintain law and order. However, unregulated police tactics, or policing guided by the principle that ends justify the means, are inconsistent with the rule of law. We recommend that *Criminal Code* section 25.1 and related sections be repealed, so that public officers are not legally justified in committing criminal offences.

Intelligence gathering is potentially more insidious to individual rights and freedoms than other types of policing, and more difficult to hold accountable. The CBA is concerned that information gathered will not necessarily be tested for its accuracy or reliability before it is entered into the security intelligence system.

Information sharing between Canada and other countries

Since September 11, 2001, Canada and the U.S. in particular have shared information at unprecedented levels. Once Canada shares information with governments that use different tactics in the so-called war on terrorism, it loses control over its use in these tactics.

In a democracy, the government must give adequate justification for the use of secret surveillance whenever it occurs, and adequate safeguards must be attached to deter abuses and protect the rights of those who may be affected by its use. The government must carefully assess existing and proposed surveillance activities, laws and technologies to ensure they are appropriate and subject to meaningful controls and independent oversight.

Oversight Mechanisms

The broad powers under the *Anti-terrorism Act* allow the government to gather information in support of intelligence-led policing and to maintain secrecy over intelligence information that forms the basis of allegations against individuals arrested under Act. The risks of abuse associated with those powers demand that there be effective oversight and accountability of Canada's intelligence and security agencies. Parliamentary oversight can play an important role in assessing overarching political issues relating to national security. We believe that an independent oversight mechanism is also needed, to address operational matters not currently covered by the Security Intelligence Review Committee (SIRC).

Non-Disclosure of Information — Canada Evidence Act, section 38.04

The *Anti-terrorism Act* added provisions to the *Canada Evidence Act* that turn section 38 applications into an absurd process. The Federal Court has no discretion to determine whether a hearing should proceed in public and whether materials before it should be made public. Secrecy is mandated throughout. Section 38 should be amended to make public the fact of an application and to ensure that proceedings are as open as possible, taking security considerations into account.

Extraordinary Investigative Powers

The government's ability to collect information is further enhanced by the investigative hearing provisions of the *Criminal Code*, execution of search warrants, and interception of private communications. Significantly, a judge may authorize the interception of private communications for investigation of a

terrorism offence without the normal necessity of being satisfied that "it would be in the best interests of the administration of justice to do so".[2]

Racial Profiling and Hate Crimes

Law enforcement authorities may detain individuals on the basis of a reasonable ground to suspect that they are involved in terrorist activities or associated with terrorists. The *Anti-terrorism Act* and other new legislation and policies have had an immediate impact on particular groups. The federal, provincial, territorial and local governments should adopt legislation, policies, regulations and procedures to define racial profiling and take concrete measures to document, sanction and prohibit it. Hate crimes must be vigorously investigated and prosecuted.

Using Immigration Law To Fight Terrorism

The *Anti-terrorism Act* has seen minimal use in an immigration context. In immigration matters, the Federal Court refers most often to the Supreme Court's definition of terrorism in *Suresh v. Canada (Minister of Citizenship and Immigration)*.[3]

More often, a security certificate is issued against a foreign national under IRPA. A Federal Court review of a security certificate issued under IRPA cannot be appealed, leaving the law in a state of uncertainty with no possibility of being sorted out by an appellate court.[4] We recommend that IRPA section 80(2) be amended to allow for an appeal from a Federal Court decision on the reasonableness of a security certificate, with leave of the Federal Court of Appeal.

In a Federal Court review of a security certificate, the government can apply for non-disclosure to the person concerned. We recommend the courts appoint an

2 Section 186(1)(a).

3 [2002] S.C.J. No. 3 (Q.L.).

4 *Immigration and Refugee Protection Act*, s. 80(2).

amicus curiae to whom confidential material would be disclosed and who could represent the interests of the person concerned.

Terrorist Financing

Offences relating to terrorist financing (*Criminal Code* sections 83.02, 83.03 and 83.04) are broad and uncertain in scope, using phrases such as "directly or indirectly", "in whole or in part", "facilitating", and "benefiting". Monitoring and reporting requirements relating to these offences are extraordinary in Canadian law, compelling non-state actors to participate in criminal investigations and information gathering strategies. The CBA expresses concern that the facilitating offence could catch lawyers providing legal advice, hampering the ability to obtain legal services and potentially violating a client's right to solicitor-client confidentiality and privilege.

Impact on Charities

Under the *Anti-Terrorism Act,* charitable activities thought until recently to be commonplace and uneventful may now make an innocent charity susceptible to:

- criminal charges for facilitating "terrorist activities" or supporting "terrorist groups."
- de-registration for suspected involvement in "terrorist activities", with the charity losing its charitable status and its directors exposed to personal liability.
- surveillance of its financial activities, potentially leading to allegations of terrorist financing.

However, the greatest impact of the *Anti-terrorism Act* may not be its direct application, but rather its indirect impact in creating fear of the "shadow of the law", even if the Act is never enforced against a charity.

We recommend that the federal government adopt "made-in-Canada" best practice guidelines, outlining requirements for charities to comply with the *Anti-terrorism Act*. The guidelines should be developed in consultation with

representatives of the charitable sector, through the Charities Advisory Committee of the Canada Revenue Agency or another similar body.

Privacy and Protection of Personal Information

Privacy is protected through the right to be secure against unreasonable search or seizure, and is fundamental to security of the person. The widespread use of technology and human sources to gather information, and the use of technology to collate and disseminate information makes the protection of private information critical to this review.

Sections 87, 103 and 104 of the *Anti-terrorism Act* amended the *Access to Information Act*, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) respectively, to permit the Attorney General of Canada to issue a certificate prohibiting disclosure of information to protect international relations or national defence or security. The Acts are inoperative for information covered by the certificate. The CBA continues to have concerns about these provisions and recommends that they be repealed. Alternatively, significant safeguards should be established.

Submission on the Three Year Review of the *Anti-terrorism Act*

I. INTRODUCTION

The Canadian Bar Association (CBA) appreciates the opportunity to contribute to the evaluation of the operation of Canada's anti-terrorism legislation, enacted with a sense of urgency just over three years ago. The CBA expressed considerable concerns when the *Anti-terrorism Act* was introduced, though we understood the urge to respond to the tragedy that had just happened in the United States. In 2001, we advocated review and repeal of any hastily enacted legislation as soon as legitimate security reasons were no longer demonstrable, and we stressed the need for independent oversight of all extraordinary powers granted to law enforcement agencies. Since September 11, 2001, the federal government has enacted or proposed other measures both explicitly and implicitly based on fear of terrorism.[5] These measures dramatically expand state powers at the expense of due process and individual rights and freedoms. Invasions on privacy and fundamental rights are creeping into Canadian law.

---

5 Examples include:

Criminal Code amendments to combat organized crime (Bill C-24) exempt police officers and police agents from liability for criminal acts.

The *Immigration and Refugee Protection Act* (IRPA) reduces rights of immigrants and refugees and diminishes fair processes to protect those rights.

Customs Act amendments (Bill S-23) permit customs officials to open mail over a certain weight, whether it is entering or leaving Canada.

Canada has implemented a number of so called "Smart Border" strategies with the U.S., many at the sub-legislative level. In addition, Canada has considered the introduction of National Identity Cards, including biometric technology linked to computer systems that cross international borders. In its April 2004 National Security Policy, *Securing an Open Society: Canada's National Security Policy*, the government indicated it would implement facial recognition biometric technology on the Canadian passport as part of the Passport Security Strategy.

The *Public Safety Act* 2002 requires airlines to provide passenger information to law enforcement agencies, which could be cross-referenced for law enforcement purposes completely unrelated to terrorism.

"Lawful access" proposals likely to be introduced in the near future will propose numerous techniques for conscripting private entities to take part in surveillance activities, possibly without meaningful oversight.

Scope of Parliamentary Review

The three-year review should go beyond the *Anti-terrorism Act*, and look at the overall impact of all expressed anti-terrorism measures, as well as measures not necessarily adopted in response to terrorism but which operate in that context. The three-year review represents an opportunity for the Government to formulate comprehensive, long-term national policy for effective law enforcement and national security. That national policy must recognize and protect individual rights and freedoms that are fundamental, and indeed, *define* Canadian democracy.

This review should consider:

- appropriate objectives for an anti-terrorism strategy, including the distinction between national security and enforcement of criminal law;
- tools required for an effective anti-terrorism strategy;
- risks associated with terrorism and objective ways to evaluate suggested risks;
- the legal, constitutional and moral standards to be protected;
- a unified, national, independent review mechanism to ensure accountability of all agencies responsible for the advancement of anti-terrorism strategies, including law enforcement and intelligence gathering.

Is There a Need for Anti-Terrorism Legislation?

A useful starting point for the review is to consider whether and why Canada needs this particular legislation. What gaps in the pre-existing legislation do the *Anti-terrorism Act* and other security-related measures fill? In our 2001 brief, the CBA provided an extensive list of laws already available to deal with terrorist threats, questioning exactly the extent of any perceived gaps.[6]

In spite of the urgency in which the *Anti-terrorism Act* was enacted, it has barely been used since 2001. The case law is restricted to *Application under section*

6 (Ottawa: CBA, 2001) at 10.

83.28 of the Criminal Code (Re),[7] examining the constitutionality of investigative hearings.

A comprehensive review addresses at least four legislative regimes: criminal law; immigration law; the law on freezing and seizing funds; and charities law.

In **criminal law**, the underlying principle is that terrorist activity should be a crime. Prior to the *Anti-terrorism Act*, the *Criminal Code* criminalized specific acts that might be committed by terrorists, but did not attempt to define "terrorist" or "terrorist activity" generally. The *Anti-terrorism Act* made terrorist activities a crime, but the law has been little used. There have been no convictions and only one person charged.[8] In situations that might be seen as a terrorist act, such as the firebombing of the United Talmud Torah School in April 2004, the law was not used.

Immigration law is where the fight against terrorism has daily practical application. People are regularly brought before immigration tribunals, for removal on allegations of membership in a terrorist group. Refugee claims are regularly scrutinized for possible rejection on the basis of participation in terrorism. Applications for permanent residence are regularly weighed taking into account possible membership in a terrorist entity. Alleged terrorists are regularly detained for removal and considered for detention release by the Federal Court.

The result is a substantial body of jurisprudence about immigration and terrorism. We see heavy use of immigration law (with no definition of terrorism) to combat terrorism outside the scope of the *Anti-terrorism Act*, combined with virtually unused criminal law (with detailed provisions dealing specifically with terrorism).

7 [2004] 2 SCR 248, (2004) 184 CCC (3d) 449 (SCC).

8 An Ottawa man, Mohammad Momin Khawaja, arrested in March 2004.

The **law on freezing and seizing funds** also raises questions about the function and utility of the *Anti-terrorism Act*. The operative law used to freeze and seize funds is the *United Nations Act*, which gives the Governor in Council authority to enact decisions of the Security Council. Canada's *United Nations Suppression of Terrorism Regulations*[9] enacted under the authority of the *United Nations Act,* require freezing funds of a long list of organizations and individuals from around the world. However, the UN Security Council Resolution 1267 Subcommittee lists only organizations and individuals belonging to or associated with the Taliban and Al-Qaeda as those whose funds states must freeze. Why, then, is the *United Nations Act* used in this context, but not the *Anti-terrorism Act*?

In this area, it is difficult to say if there are cases that the current law is not addressing. Freezing funds of terrorist entities and individuals is not reported publicly. Have any funds been frozen in Canada under the *United Nations Suppression of Terrorism Regulations*? If not, does fundraising in Canada not end up in the hands of terrorists, in spite of allegations to the contrary? Or is the UN law not working and in need of revision? If funds have been frozen, why is no activity reported under the *Anti-terrorism Act*? If a law is required, what changes would make the *Anti-terrorism Act* more effective?

The need for anti-terrorism provisions in **charities law** is difficult to speak to because it functions in a negative way. Charitable numbers are not given to terrorist entities. Rather, the law addresses expenditures by charities on terrorist entities. Again, lack of integration with other areas of law results in anomalies.

The CBA acknowledged from the beginning that balancing individual rights and freedoms would likely be required to advance national security. However, experience has shown that the compromise is not demanded equally of all who are theoretically made more secure by the law. Certain religious and ethnic groups have been targeted more often since the *Anti-terrorism Act* came into force. This

9 SOR/2001-360.

is the time to assess whether anti-terrorism legislation is needed in Canada, and if so, how to make it effective without undue compromise of individual rights and freedoms.

II. CANADA'S DEMOCRATIC FRAMEWORK

Rule of Law and Charter of Rights

The laws, values and constitutionally guaranteed rights and freedoms that define Canadian democracy must guide an effective analysis of Canada's anti-terrorism strategy. Recognizing the rule of law as an overarching principle, the *Charter* rights and freedoms of particular importance to this review are:

- freedom of thought, belief, opinion, expression, conscience, religion, peaceful assembly and association (section 2)
- security of the person, including privacy (section 7)
- equal protection and benefit of the law without discrimination (section 15)
- security against unreasonable search or seizure and arbitrary detention (section 8)
- right to a fair trial and the presumption of innocence (section 11).

The rule of law is one of the organizing principles of democratic society. In *Reference Re Secession of Quebec*, the Supreme Court of Canada held that "at its most basic, the rule of law…provides a shield for individuals from arbitrary state action."[10] Law must not be used for an arbitrary or capricious purpose; limits on individual rights must be reasonable and demonstrably justified; laws must clearly delineate an area of risk, provide fair notice to individuals, and limit the discretion of law enforcement; laws must not be a "standardless sweep".[11]

10 [1998] 2 SCR 217 at para 70.

11 *R.* v. *Morales*, [1992] 3 SCR 711.

Parliament's prerogative to enact criminal law is not absolute. As stated by Dickson C.J. in *R. v. Oakes*, "In Canada, we have tempered Parliamentary supremacy by entrenching important rights and freedoms in the *Constitution*."[12]

At the same time, rights recognized by the *Charter* are not unqualified. Thus, again in *Oakes*, Dickson C.J. held:

> The rights and freedoms guaranteed by the *Charter* are not, however, absolute. It may become necessary to limit rights and freedoms in circumstances where their exercise would be inimical to the realization of collective goals of fundamental importance.[13]

This is reflected in sections 1 and 7 of the *Charter*:

> 1. The Canadian *Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to the limits prescribed by law as can be demonstrably justified **in a free and democratic society**.
>
> 7. 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.

Oakes stated the significance of the phrase "free and democratic society":

> Inclusion of these words as the final standard of justification for limits on rights and freedoms refers the court to the very purpose for which the *Charter* was originally entrenched in the Constitution: Canadian society is to be free and democratic. The court must be guided by the values and principles essential to a free and democratic society which I believe embody, to name but a few, respect for the inherent dignity of the human person, commitment to social justice and equality, accommodation of a wide variety of beliefs, respect for cultural and group identity, and faith in social and political institutions which enhance the participation of individuals and groups in society. The underlying values and principles of a free and democratic society are the genesis of the rights and freedoms guaranteed by the *Charter* and the ultimate standard against which a limit on a right or freedom must be shown, despite its effect, to be reasonable and demonstrably justified.[14]

Democracy creates an inescapable tension between collective goals, such as national security, and individual rights. Attaining collective goals will often necessitate limits on an individual right or freedom. Within the context of the criminal justice system, the Court has described the coexistence between state

---

12 [1986] 1 SCR 103 at 125, (1986) 24 CCC (3d) 321 (SCC) at 338.

13 *Ibid.* at 346.

14 *Ibid.*

interests and individual rights as "a delicate balancing to achieve a just accommodation between the interests of the individual and those of the state in providing a fair and workable system of justice."[15]

The U.K. House of Lords recently considered Article 5(1) of the *European Convention on Human Rights*, [16] given effect in the U.K. by the *Human Rights Act 1998*.[17] Article 15 of the European Convention gives member states a limited right to derogate from some articles.[18]

The U.K. Parliament speedily enacted Part 4 of the *Anti-terrorism, Crime and Security Act 2001* after the events of September 11. It followed with the *Human Rights Act 1998 (Designated Derogation) Order 2001* (SI 2001/3644), exempting the anti-terrorism legislation from the human rights protections. The U.K. was the only country of 45 in the Council of Europe to derogate from article 5.

The appellants argued the long libertarian tradition of English law, dating back to the *Magna Carta*, given effect in the ancient remedy of *habeas corpus* declared in the *Petition of Right 1628*. The court acknowledged that British constitutional history provided an exceptional power to derogate from those rights:

> There have been times of great national emergency in which *habeas corpus* has been suspended and powers to detain on suspicion conferred on the government. It happened during the Napoleonic Wars and during both World Wars in the twentieth century. These powers were conferred with great misgiving and, in the sober light of retrospect after the emergency had passed, were often found to have been cruelly and unnecessarily exercised.[19]

The appeals were allowed and the *Human Rights Act 1998 (Designated Derogation) Order 2001* quashed.

---

15 *R.* v. *Harrer*, [1995] 3 SCR 562 at para 14.

16 Rome 4 November 1950. Article 5(1) states that: "Everyone has the right to liberty and security of person".

17 1998 Chapter 42. See, *A (FC) and others (FC)* v. *Secretary of State for the Home Department*, [2004] UKHL 56.

18 *Derogation in time of emergency*

1. In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.

19 *Supra* note 17 at para 89.

International Obligations

It is extremely difficult to trace domestic implementation of various anti-terrorism conventions to which Canada is a party, in the *Criminal Code* or other statutes. Transparency in how the anti-terrorism agenda in multilateral treaties is reconciled with Canadian law would enhance the quality and effectiveness of this review. We see the potential for conflict between Canada's obligations under international law and under the *Charter of Rights* or otherwise.

An August 2004 UN report on *Measures to Eliminate International Terrorism*[20] lists 22 global or regional treaties on international terrorism. Ten of these ratified by Canada were incorporated by reference into the definition of "terrorist activity" in the *Anti-terrorism Act*.[21]

RECOMMENDATION

The Canadian Bar Association recommends that the federal government:

- **Indicate clearly the adoption of Canada's obligations under international conventions and instruments in Canadian domestic law.**
- **List in annual reports on the *Anti-terrorism Act* cases applying Canada's obligations under international conventions and instruments.**

---

20 August 5, 2004, UN General Assembly: Report of the Secretary General (A/59/210), prepared pursuant to General Assembly resolution 50/53, Dec 1995. <http://daccessdds.un.org/doc/UNDOC/GEN/N04/452/28/PDF/N0445228.pdf?OpenElement>

21 See Canada: *Anti-terrorism Act*, SC 2001, c. 41, section 4 (Definitions: "terrorist activity," provisions in the *Criminal Code* amendments, Part II, 1, section 83.01, referencing: the *Convention for the Suppression of Unlawful Seizure of Aircraft (1970); the Convention for the Suppression of Unlawful Acts against the Safety of Civil Action* (1971); the *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents* (1973); the International *Convention against the Taking of Hostages* (1979); the *Convention on the Physical Protection of Nuclear Material* (1980); the *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Action supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (1988); the *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Aviation* (1988); the *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf* (1988); the *International Convention for the Suppression of Terrorist Bombings* (1997); and the *International Convention for the Suppression of Terrorist Financing* (1999).

III. DEFINING TERRORISM

Three years ago, CBA expressed several concerns about the attempts to define terrorism in Bill C-36. Effective anti-terrorism legislation must identify with some precision what will be considered "terrorist activity". Imprecision opens the door to subjective interpretation and arbitrary application of the law, which can too readily lead to abuses, discrimination and persecution rather than protection of national security interests.

The CBA expressed concern that the threshold definition of "terrorist activity" in Bill C-36 was so expansive that it would encompass legitimate protest, along with behaviour that was criminal but not terrorist. We continue to believe that the definition in the *Anti-terrorism Act* is too wide and too vague. In our view, a consistent definition should be used in all Canadian legislation pertaining to terrorism. We suggest the definition in the United Nations *Convention for the Suppression of the Financing of Terrorism*.[22]

RECOMMENDATION

The CBA recommends that terrorist activities be defined consistently in all Canadian laws relating to terrorism, adopting the definition in the UN *Convention for the Suppression of the Financing of Terrorism*:

> **Any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.**

22 Adopted by the General Assembly of the United Nations on 9 December 1999 (entered into force on 10 April 2002).

Under the *Anti-terrorism Act*, "terrorist activity" includes conspiracy, attempts or threats, as well as being an accessory after the fact or counseling. The act must be "committed in whole or in part for political, religious or ideological purposes, objectives or causes". This goes beyond Canada's international obligations, which require only that the acts contemplated by anti-terrorism legislation are "under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature".[23]

"Terrorist group" is defined in *Criminal Code* section 83.01(1) as:

> (a) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or
>
> (b) a listed entity,
>
> and includes an association of such entities.

Again, the breadth of the definition captures a host of legitimate entities that are not the intended target. For example, a legitimate charity could be a "listed entity" if the nature and location of its international humanitarian work led the Government to believe on "reasonable grounds" that the charity had knowingly carried out, attempted to carry out, participated in, or facilitated a terrorist activity. Coupled with the definition of "facilitate", the definition of "terrorist group" could apply to charitable organizations with no direct or indirect involvement or intent to participate in terrorist activities.

Criminal Code section 83.19(2) clarifies the scope of "facilitating"[24]:

> For the purposes of this Part, a terrorist activity is facilitated whether or not;
>
> (a) the facilitator knows that a particular terrorist activity is facilitated;
>
> (b) any particular terrorist activity was foreseen or planned at the time it was facilitated; or
>
> (c) any terrorist activity was actually carried out.

23 UN Security Council Resolution 1566 para 3.

24 See also *Criminal Code* sections 83.01(2), 83.19(2).

Any entity making it easier for another to commit a terrorist activity could itself be a terrorist group, regardless of whether a particular terrorist act was facilitated or foreseen and even if no terrorist act actually occurred. For example, the services of Internet or wireless service providers, cell phone manufacturers and car rental companies make it easier for terrorist groups to conduct their activities, but they would not know the specific acts inadvertently aided. Certainly, it would be unreasonable to call a car rental company a terrorist group because they facilitated the Oklahoma City bombing. Criminal intent should be required.

While law enforcement agencies may well agree that this is an absurd extension of the law, the net is nonetheless cast to give them discretion to pursue individuals or organizations. The wide scope of "facilitating" means that individuals and organizations may unwittingly violate the strict letter of the criminal law, and must trust the government to enforce the law only against "real criminals". In our view, such an approach is inimical to Canadian criminal law.

RECOMMENDATION

The CBA recommends that the *Criminal Code* be amended to require the Crown to prove criminal intent to find anyone guilty of a terrorist offence.

The expansive definition of participating or contributing in section 83.18(3) includes providing or offering to provide a skill or expertise for the benefit of a terrorist or terrorist group. Lawyers representing accused terrorists could be seen as providing a skill or an expertise for the benefit of the terrorist group. In determining participation or contribution, the court may consider frequent association with those in the terrorist group or receipt of any benefit from the terrorist group – section 83.18(4). This could also include defense counsel.

RECOMMENDATION

The CBA recommends that lawyers providing legal services to those accused of terrorist offences be specifically excluded

from the ambit of section 83.18, dealing with participation in or contribution to an activity of a terrorist group.

IV. LAW ENFORCEMENT AND INTELLIGENCE GATHERING TOOLS

Requirement for Effective Law Enforcement

Canadian democracy rests, in part, on the existence of effective law enforcement and intelligence gathering. Terrorist activity has the potential to destabilize or destroy the very institutions and values that define our democracy.

Effective law enforcement and intelligence gathering require certain tools and access to information. These include search warrants, authorization to intercept private communications, access to data from other government agencies and international sources, and information from informants. Based on information from various sources, government agencies can assess threats, detect threats to national security or criminal acts, prevent breaches of national security or crimes, and gather evidence in support of criminal prosecutions.

While individual rights and freedoms depend to some extent upon stable and democratic government institutions and the rule of law, the objectives of the government may, at times, be antithetical to those rights and freedoms.

The Supreme Court of Canada considered this tension in *R. v. Mentuck,*[25] looking at the constitutional validity of the publication bans on police operational methods:

> A fundamental belief pervades our political and legal system that the police should remain under civilian control and supervision by our democratically elected officials; our country is not a police state. The tactics used by police, along with other aspects of their operations, is a matter that is presumptively of public concern.

25 [2001] 3 SCR 442.

> In my view, a publication ban that restricts the public's access to information about the one government body that publicly wields instruments of force and gathers evidence for the purpose of imprisoning suspected offenders would have a serious deleterious effect. There is no doubt as to how crucial the role of the police is to the maintenance of law and order and the security of Canadian society. But there has always been and will continue to be a concern about the limits of acceptable police action. The improper use of bans regarding police conduct, so as to insulate that conduct from public scrutiny, seriously deprives the Canadian public of its ability to know of and be able to respond to police practices that, left unchecked, could erode the fabric of Canadian society and democracy. [26]

Similarly, in *R. v. Mack,* the Court held:

> It is a deeply ingrained value in our democratic system that the ends do not justify the means. In particular, convictions may, at times, be obtained at too high a price. This proposition explains why as a society we insist on respect for individual rights and procedural guarantees in the criminal justice system…many of the rights in ss.7-14 of the *Charter* relate to norms for the proper conduct of criminal investigations and trials, and courts are called on the ensure that these standards are observed.[27]

Still more recently, and specifically in the context of the constitutional validity of *Criminal Code* section 83.28, the investigative hearing provision, Iacobucci and Arbour JJ. made the following remarks in *Application under section 83.28 of the Criminal Code (Re)*:[28]

> The challenge for democracies in the battle against terrorism is not whether to respond, but rather how to do so. This is because Canadians value the importance of life and liberty, and the protection of society through respect for the rule of law. Indeed, a democracy cannot exist without the rule of law.
>
> . . .
>
> Although terrorism necessarily changes the context in which the rule of law must operate, it does not call for the abdication of law. Yet, at the same time, while respect for the rule of law must be maintained in response to terrorism, the Constitution is not a suicide pact, to paraphrase Jackson J.: Terminiello v. Chicago (City), 377 U.S. 1 (1949), at p.37 (in dissent).

. . .

---

26 *Ibid.* at para 50-51.

27 [1988] 2 SCR 903, (1988) 44 CCC (3d) 513 (SCC) at 539.

28 *Supra* note 7 at paras 5-7.

Consequently, the challenge for a democratic state's answer to terrorism calls for balancing of what is required for an effective response to terrorism in a way that appropriately recognizes the fundamental values of the rule of law. In a democracy, not every response is available to meet the challenge of terrorism.

Similar principles are found in U.S. jurisprudence. In *Hamdi v. Rumsfeld*,[29] the U.S. Supreme Court considered the legality of the detention of "enemy combatants". In finding the detention illegal to the extent that due process required an opportunity for review, Justice O'Connor wrote: "…war is not a blank check for the President when it comes to the rights of the Nation's citizens."

An effective police force is essential to maintain law and order. However, unregulated police tactics, or policing guided by the principle that ends justify the means is inconsistent with and detrimental to the rule of law. Parliament has gone so far as to enshrine an exemption for police officers and their agents who commit certain illegal acts that would otherwise constitute a criminal offence.[30]

RECOMMENDATION

The CBA recommends that *Criminal Code* section 25.1 and related sections be repealed, so that public officers are not legally justified in committing criminal offences.

Intelligence Gathering

Intelligence gathering entails the collection, evaluation, analysis and dissemination of information, generally with the goal of stopping illegal and harmful occurrences before they happen. While important, intelligence gathering is potentially more insidious to individual rights and freedoms than other types of policing, and more difficult to hold accountable.

29 June 28, 2004, Docket # 03-6696 (US Supreme Court).

30 *Criminal Code* section 25.1 *et seq*, SC 2001, c. 32.

In his testimony to the Arar Commission,[31] the RCMP Deputy Commissioner referred to "intelligence-led policing" as the RCMP's new focus. Their mission is to create a national program for the management of criminal information and intelligence to allow the RCMP to detect and prevent crime with an organized, serious or national security dimension in Canada, or internationally as it affects Canada. "Information" is defined as "unprocessed data of every description which may be used in the production of intelligence." The RCMP and CSIS share common objectives, so the agencies integrate and share information.[32]

The RCMP is, therefore, not solely engaged in collecting evidence to support the investigation and prosecution of crimes that have already occurred. Their mission now is to gather information to predict and prevent criminal activity. The RCMP interacts with a number of agencies including CSIS, Foreign Affairs Canada, the Communications Security Establishment, the Department of National Defence, Citizenship and Immigration Canada, FINTRAC, municipal and provincial police forces and U.S. and other foreign agencies.[33] Information is shared amongst a vast number of agencies, in Canada as well as other countries.

The definition of terrorism and the scope of terrorism-related offences make it probable that the information collected is vast. The Deputy Commissioner's testimony provided an example: if the police are targeting X in an investigation, and during surveillance X is seen occasionally speaking to Y, Y is then entered onto the security intelligence information system. The field officer conducting the surveillance need not receive authority to enter Y into the data bank and, once entered, information in the system may be shared with U.S. law enforcement agencies. As of November 2004, 35 entities were listed for purposes of the anti-terrorism offences in the *Criminal Code*. It is therefore likely that the RCMP is

31 The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (the Arar Commission), June 30, 2004. <http://ararcommission.ca>

32 The Deputy Commissioner spoke of a need for a "sophisticated process of centralized coordination" and an integrated approach between intelligence and enforcement.

33 "The RCMP and National Security", a Policy Review paper prepared for the Arar Commission, *supra* note 31.

actively seeking information that might identify the principals of those entities, persons who facilitate or assist those entities, or persons believed to be associated with those entities.

The information will not necessarily be tested for its accuracy or reliability before it is entered into the security intelligence system. It is only information, as opposed to evidence that might be adduced against an individual in a criminal prosecution. An individual whose name, license plate, photograph, residential address, or family members have been entered into the data bank will likely not know that this has occurred. Even if they know that personal information has been collected, they will be unlikely to determine details, to correct inaccurate or false information, or to have information removed from the system.

The RCMP has considered the accountability problems associated with this type of information gathering:

> The courts serve an extremely important third party accountability function for police agencies. This role arises primarily out of the criminal trial process. In the course of a trial, the activities of a police force in investigating and apprehending an individual will be subject to the scrutiny of the courts. However, in regard to crimes related to national security, there is a risk that the opportunity for such judicial scrutiny will not often occur.[34]

This issue was considered in the BC Information and Privacy Commissioner's report *Privacy and the USA Patriot Act*.[35] The Commissioner found:

> Perhaps the most troubling theme to emerge from the submissions and from our analysis is the blurring of the lines that have traditionally separated the state's national security and law enforcement functions.[36]

The blurring of lines was found to be associated with "a marked increase in the breadth and intensity of state surveillance".[37]

---

34 *Ibid.* at 33.

35 *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (Vancouver: Information & Privacy Commissioner for British Columbia, October 2004).

36 *Ibid.* at 29.

37 *Ibid.*

Information Sharing between Canada and Other Countries

Since September 11, 2001, Canada and the U.S. in particular have shared information at unprecedented levels. Deputy Prime Minister McLellan has stated that there is now a seamless flow of information between Canada and the U.S.[38] Top CSIS officials have confirmed that cross-border cooperation has increased immensely since 2001.

The foreseeable and unforeseeable consequences of sharing information gives rise to grave concerns. The case of Maher Arar is the most publicized example of the dangers of unrestricted information sharing. Once Canada shares information with governments that use different tactics in the so-called war on terrorism, it loses control over its use in these tactics. While we recognize the need for Canada to share information with U.S. intelligence agencies, the Arar case and others raise serious questions about the need for appropriate safeguards.[39]

The impact of information sharing is heightened by the broad powers of arrest and detention under the *Anti-terrorism Act*. Individuals may be held on information emanating solely from intelligence or law enforcement agencies in another country. The reliability of the information needn't be tested, in particular, whether it was obtained by means of torture. Another concern is the mandated secrecy that goes along with receiving information from a foreign jurisdiction. As a part of information sharing, Canada is obligated to guarantee that the information will not be shared without permission of the foreign jurisdiction.[40] This affects the rights of those in Canada to know the case against them and to

38 Deputy Prime Minister, Ann McLellan, "Speaking Notes" (Address to the Federation of Canadian Municipalities at the 67th Annual conference and Municipal Expo, Edmonton, Alberta, May 28 2004).

39 Mr. Arar and at least four other Canadians have stated that they were detained and in three cases tortured where the information that led to their arrest is believed to have been received from Canadian security agencies: Ahmad El-Maati; Abdullah Almalki; Muayyed Nureddin; and Kassim Mohammed.

40 This is an admittedly grey area. On the one hand, CSIS claims they receive information from Syria on the understanding that they cannot share it without Syria's consent. On the other hand, Canadian agencies send dossiers to the U.S. and other countries with no such assurances.

defend themselves where Canadian authorities seek to use the information in proceedings in Canada.

In a democracy, the government must give adequate justification for the use of secret surveillance whenever it occurs, and adequate safeguards must be attached to deter abuses and protect the rights of those who may be affected by its use. The government must carefully assess existing and proposed surveillance activities, laws and technologies to ensure they are appropriate and subject to meaningful controls and independent oversight.

In our view, there must be controls on sharing information to ensure it remains subject to the protections guaranteed under the *Charter*. This is especially true when contemplating sharing with regimes that do not respect human rights. If the government continues to share personal information gathered in Canada, it should do so only if confident that protections applicable in Canada will continue to apply wherever the information is transferred.

RECOMMENDATION

The CBA recommends that the federal government:

1. **enact regulations with safeguards for sharing information with regimes that do not respect human rights, to ensure that the information is shared in a manner that does not put Canadian citizens at risk;**
2. **share raw intelligence information with the caveat that the information has not been proven and that it should be acted on only with caution;**
3. **affirm that it is unacceptable for Canadian citizens to be deported from other countries to undemocratic regimes or regimes that engage in torture, and insist that Canadian citizens instead be returned to Canada; and**

4. **establish an independent compensation mechanism to which Canadian citizens suffering harm because of information shared without proper safeguards can apply for compensation.**

Oversight Mechanisms

In an August 2004 address to the International Commission of Jurists (ICJ), UN High Commissioner for Human Rights Louise Arbour stated that, over the long term, "a commitment to uphold respect for human rights and rule of law will be one of the keys to success in countering terrorism — not an impediment blocking our way." While stressing that States have not only the right, but also the duty to secure the right to life and other human rights through effective counter-terrorism measures, she also highlighted the central role of the judiciary in reviewing such measures taken by Governments.

> Put bluntly, the judiciary should not surrender its sober, long-term, principled analysis of issues to a call by the executive for extraordinary measures grounded in information that cannot be shared, to achieve results that cannot be measured. [41]

Measures to ensure transparency and accountability can minimize injustice, discrimination and loss of faith in our justice system that is likely when state power goes unchecked. An effective civilian oversight mechanism can ensure that public servants remain accountable to the people they serve. It can prevent serious breaches, with the potential attendant costs for wrongful convictions and imprisonment, appeals, mistrials and public inquiries.

The Commissioner for the RCMP Public Complaints Commission has said that "[f]or the first time in Canadian history, we have passed a law creating crimes involving terrorism that compel police to investigate the political, religious or

41 Cited in United Nations Secretary-General's report "Protecting Human Rights and Fundamental Freedoms while Countering Terrorism", October 2004 (A/59/404) at 5.

ideological beliefs of individuals".[42] "Intelligence-led policing" authorizes law enforcement officials to anticipate, predict and prevent crimes and security threats based on information gathered in advance of criminal activities. Court oversight is limited in this national security context, given the secrecy involved and the focus on prevention, rather than prosecution.

Regrettably, it is not uncommon for police to violate constitutionally guaranteed rights in the investigation and enforcement of criminal law. Without the accountability that comes from a criminal trial, those violations would go undetected. Worse, if an investigative agency gathers information knowing that there will not be a criminal charge, there may be even less incentive to respect guaranteed rights and freedoms.

Several federal agencies engage in national security activities[43] and some have a mechanism for civilian oversight. The mechanisms differ in their independence, their powers, whether they are complaint driven or self initiated, whether they issue orders or recommendations, what access they have to information, how they are resourced, and how and to whom they report.[44]

In her November 2003 report, the Auditor General assessed the mechanism of review associated with agencies involved in the collection of intelligence and found that the powers to review the different agencies vary significantly. She recommended that:

> The government should assess the level of review in reporting to Parliament for security and intelligence agencies to ensure that agencies exercising intrusive powers are subject to levels of external review and disclosure proportionate to the level of intrusion.

---

42 Shirley Heaffey, Chair, Commission for Public Complaints Against the RCMP, "The Need for Effective Civilian Oversight of National Security Agencies in the Interest of Human Rights" (Speech delivered to the University of Ottawa, Faculty of Law, Ottawa, Ontario, October 2003).

43 Police review bodies include the Commission for Public Complaints Against the RCMP, the Military Police Complaints Commission, and complaint-based review commissions in all provinces and territories except PEI. Review mechanisms for security agencies include the Security Intelligence Review Committee for CSIS, the CSE Commissioner for the *Communications Security Establishment.*

44 *Supra* note 32 at 20.

> The broad powers under the Anti-terrorism Act allow the government to gather information in support of intelligence-led policing and to maintain secrecy over intelligence information that forms the basis of allegations against individuals arrested under Act. The risks of abuse associated with those powers demand that there be effective oversight and accountability of Canada's intelligence and security agencies. It is now more important than ever that Canadian security and intelligence agencies comply with their respective mandates, and with strict controls over how they collect and analyze intelligence information.

With increased cooperation between agencies, the need for a single oversight committee with power to review the activities of all agencies involved is necessary as it may be impossible to assess the reasonableness of one agency's activities without reviewing the activities of another. Even if each agency or department has an adequate mechanism for accountability, a patchwork system will not ensure that laws, policies, practices and objectives are operating — individually and in their cumulative effect — in accordance with the standards of law, morality, and constitutional rights and freedoms. A comprehensive, independent body can ensure overall accountability.

The Government recently proposed a national security committee of Parliamentarians. The mandate of the Parliamentary Committee would be to "review the security and intelligence apparatus in Canada, and the ability of departments and agencies engaged in security and intelligence activities to fulfill their responsibilities."[45]

Parliamentary oversight can play an important role in assessing overarching political issues relating to national security. We believe that an independent oversight mechanism is also needed, to address operational matters not currently covered by the Security Intelligence Review Committee (SIRC).

---

45 Public Safety and Emergency Preparedness Canada, Press Release and Backgrounder, "Deputy PM details Proposed Model for National Security Committee of Parliamentarians" (4 April 2005). http://www.psepcsppcc.gc.ca/publications/news/2005/20050505-3.

RECOMMENDATION

The CBA recommends the establishment of an independent oversight mechanism for all security matters not covered by SIRC.

Non-Disclosure of Information — *Canada Evidence Act* section 38.04

The *Anti-terrorism Act* added provisions to the *Canada Evidence Act* that turn section 38 applications (international relations and national defence and national security) into an absurd process. The Federal Court has no discretion to determine whether a hearing should proceed in public and whether materials before it should be made public. Secrecy is mandated throughout. The fact that notice has been given to the Attorney General or that a section 38 application has been commenced cannot be disclosed.[46]

Under subsection 38.13(5), even if the Court orders information or documents to be made public, the government reserves the right to override the Court. This renders the Court's review function pointless.

The Chief Justice of the Federal Court has outlined serious problems with section 38.04 of the *Canada Evidence Act,* because it denies public access to the review of the government's objections to disclosure.[47] In the Arar Commission of Inquiry, for example, Mr. Arar was not privy to government objections to disclosure until days later and only after the court ruled he should be considered an interested party. When advised of the application, his counsel was told that the information could not be shared with anyone else. The notice of application was confidential until the government consented to its release.

46 *Canada Evidence Act*, sections 38.02, 38.04(4) and 38.12.

47 *Ottawa Citizen Group Inc.* v. *Canada (AG) et al*., [2004] FC 1052 (Almalki).

In *Ottawa Citizen Group Inc. v. Canada (Attorney General),*[48] Chief Justice Lufty aptly expressed the judiciary's understandable frustration with the legislated secrecy under the Act:

> *Post Scriptum*: "Too much secrecy?"
>
> 34 For some twenty years now, Federal Court hearings under section 38 have been in private: S.C. 1980-81-82, c. 111, section 4, (Schedule III). The amendments enacted in the anti-terrorism legislation have added to the secrecy shrouding a section 38 proceeding. This application raises some examples of the difficulties presented by the secrecy requirements.
>
> 35 Under the current law, no one is to disclose that a notice of application under section 38 has been filed with the Federal Court: paragraph 38.02(1)(c). Put simply, not even the Court can acknowledge publicly that it is seized of a section 38 proceeding. This can lead to unintended, even absurd, consequences.
>
> 36 In this case, statements were made in open sessions of the Ontario Court of Justice in late November and December 2003 acknowledging that the section 487.3 proceeding would be suspended to permit the making of this section 38 application. I know of no impediment prohibiting the publication of this information by the media. I choose not to comment on other public statements which may have been inconsistent with subsection 38.02(1).
>
> 37 This section 38 application was filed on January 5, 2004. From the outset, this Court could not acknowledge whether the application had been made, not even to a person who would have reasonably known this to be so from the public information in the Ontario Court of Justice.
>
> 38 There may be an exceptional case where the secrecy envisaged in section 38.02 may be warranted. In the more usual situation, however, where secret information is in issue, the necessity of a section 38 proceeding is made known publicly before the person presiding over the tribunal or court hearing. The Federal Court is required by section 38 to keep secret a fact which has been referred to publicly in the court or tribunal from which the proceeding emanates. It is unlikely that Parliament could have intended that the drafting of section 38 would result in such a consequence.
>
> . . .
>
> 40 In authorizing the disclosure of the existence of this proceeding and the contents of the notice of application, the Attorney General of Canada was doing so in the sole exercise of his discretion. His authorization, in my respectful view, simply recognized the obvious. Anyone attending the proceedings before Justice Dorval in the Ontario

48 [2004] FCJ No 1303.

> Court of Justice would understand that the matter had been referred to this Court. There was no secret information in the notice of application. This same reality applies to most other section 38 proceedings. The Attorney General of Canada is likely to participate in all section 38 proceedings: section 38.04. It is unusual that a party to the litigation should be the sole arbiter to authorize the disclosure of information which is or should be public. A court should be seen as having reasonable control over its proceedings in the situation I have just described.
>
> 41 In the same vein, once the applicants had been authorized to make public the existence of this proceeding and the notice of application, the Federal Court was placed in the invidious position of maintaining confidentiality with respect to its records where one of them, the notice of application, could be in the public domain. This is because subsection 38.12(2) requires that the court records relating to the hearing be confidential. It is the breadth of the provision that appears to cause this difficulty.
>
> . . .
>
> The Supreme Court of Canada, in its recent consideration of another provision of the *Anti-terrorism Act*, has reiterated the importance of the public's access to court proceedings. The open court principle is a cornerstone of our democracy and "... is not lightly to be interfered with": Vancouver Sun (Re), [2004] S.C.J. No. 41, 2004 SCC 43 at paragraphs 23-27. Section 38 is the antithesis to this fundamental principle.

We have serious questions about the constitutional validity of many of these provisions. Similar provisions in the *Privacy Act* have already been struck down. In *Ruby v. Canada,* the Court held that a provision similar to section 38.11 of the *Canada Evidence Act* violates section 2(b) of the *Charter* and cannot be saved by section 1:

> The existence of this judicial practice makes clear, though, that the requirement that the entire hearing of a section 41 application or appeal therefrom be heard in camera, as is required by section 51(2)(a), is too stringent. The practice endorsed by the Solicitor General and courts alike demonstrates that the section is overbroad in closing the court to the public even where no concern exists to justify such a departure from the general principle of open courts. [49]

49 [2002] 4 SCR 3 at para 59.

RECOMMENDATION

The CBA recommends that:

1. ***Canada Evidence Act* section 38 *et seq.* be amended to make public the fact of an application to the Court, and to ensure that proceedings are open to the public to the greatest extent possible taking security considerations into account.**
2. **section 38.06 be amended to preclude the use of summaries of evidence in criminal proceedings.**

Extraordinary Investigative Powers

The government's ability to collect information is further enhanced by the investigative hearing provisions of the *Criminal Code*, execution of search warrants, and interception of private communications. Significantly, a judge may authorize the interception of private communications for investigation of a terrorism offence without the necessity of being satisfied that "it would be in the best interests of the administration of justice to do so".[50] Further, the statutory requirement that written notice be given within 90 days to a person who was the object of interception may be extended up to three years. Though there may sometimes be investigative concerns that justify not giving notice for three years, notice is a component of accountability and delay in giving notice results in diminished accountability.

While the Court upheld the validity of investigative hearings under section 83.28 in *Application under section 83.28 of the Criminal Code (Re),*[51] other findings are relevant to this review. First, the majority noted, "the international scope of terrorism activities and the international ambit of terrorism investigation raise grave concerns about potential uses of information gathered pursuant to section

50 Compare *Criminal Code* section186(1)(a).

51 *Supra* note 7.

83.28(10)." [52] Secondly, they affirmed the principle that openness "is integral to the public confidence in the justice system".[53]

Justices Binnie, LeBel and Fish JJ. (in dissent) found that the Crown's attempt to use section 83.28 in the course of a criminal prosecution, and in relation to a Crown witness, was "an abuse of the extra-ordinary powers granted under the *Anti-terrorism Act*".[54] Similarly, in the Air India prosecution, the trial judge ruled that late disclosure and the failure to disclose materials to the defence resulted in a breach of the accused's rights guaranteed by section 7 of the *Charter*".[55] These findings point to the potential for misuse of the extraordinary powers.

V. DISTINGUISHING CRIMINAL LAW AND NATIONAL SECURITY

Despite overlapping objectives and coordination amongst policing and information gathering agencies, we believe that it is critical to maintain the distinction between "national security" and "criminal law". While criminal law contributes to national security in a general sense, the objectives of criminal law and national security are different. Procedural protections that might be set aside for pressing matters of national security are created precisely so that people accused of criminal actions are guaranteed certain fundamental safeguards.

The Supreme Court recognized this distinction in *Application under section 83.28 of the Criminal Code (Re),* considering the constitutional validity of *Criminal Code* section 83.28 (investigative hearings). Writing for the majority, Iacobucci and Arbour JJ. held:

> It was suggested in submissions that the purpose of the Act should be regarded broadly as the protection of "national security". However, we believe that this characterization has the potential to go too far and would have implications that far outstrip legislative intent. The discussions

52 *Ibid*. at 74.

53 Re Vancouver Sun, [2004] 2 SCR 332, (2004)184 CCC (3d) 515 at para 75.

54 *Ibid.* at para 112.

55 *R.* v. *Malik* (2004), BCSC 1309 (docket #CC010287) at para 25.

> surrounding the legislation, and the legislative language itself clearly demonstrate that the Act purports to provide means by which terrorism may be prosecuted and prevented. As we cautioned above, *courts must not fall prey to the rhetorical urgency of a perceived emergency or an altered security paradigm.* While the threat posed by terrorism is certainly more tangible in the aftermath of global events such as those perpetrated in the United States, and since then elsewhere, including very recently in Spain, we must not lose sight of the particular aims of the legislation. Notably, the Canadian government opted to enact specific criminal law and procedure legislation and did not make use of exceptional powers, for example under the *Emergencies Act*, R.S.C. 1985, c.22 (4th Supp), or invoke the notwithstanding clause at s.33 of the *Charter*. *(Emphasis added)*:[56]

Similarly, Binnie J. wrote (at para.116):

> The danger in the "war on terrorism" lies not only in the actual damage the terrorists can do to us but what we can do to our own legal and political institutions by way of shock, anger, anticipation, opportunism or overreaction.

VI. USING IMMIGRATION LAW TO FIGHT TERRORISM

Use of the *Anti-terrorism Act*

The *Anti-terrorism Act* has seen minimal use in an immigration context. It is referred to in only a few decisions, often only to note that its definition gives additional guidance on the meaning of terrorism. In immigration matters, the Federal Court refers most often to the Supreme Court's definition of terrorism in *Suresh v. Canada (Minister of Citizenship and Immigration)*:[57]

> In our view, it may safely be concluded, following the International Convention for the Suppression of the Financing of Terrorism, that "terrorism" in section 19 of the [Immigration and Refugee Protection] Act includes any "act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act". This definition catches the essence of what the world understands by "terrorism". Particular cases on the fringes of terrorist activity will inevitably provoke disagreement. Parliament is not

56 *Supra* note 7 at para 38.

57 [2002] SCJ No 3 (QL).

> prevented from adopting more detailed or different definitions of terrorism. The issue here is whether the term as used in the *Immigration Act* is sufficiently certain to be workable, fair and constitutional. We believe that it is.

In subsequent cases relating to terrorism in the immigration context, the Federal Court held that any departure from the definition in *Suresh* will be set aside.

As the *Anti-terrorism Act* is used so infrequently in the immigration context, the mechanisms in the *Immigration and Refugee Protection Act* (IRPA) for finding foreign nationals and permanent residents inadmissible on security related grounds seem to be considered adequate to ensure the safety of Canadian citizens and others residing in this country.

In *Fuentes v. Canada (Minister of Citizenship and Immigration),*[58] the applicant had been found inadmissible under section 19(1)(f)(iii)(B) of the *Immigration Act.*[59] The section prevented admission to Canada if there were reasonable grounds to believe the applicant was a member of an organization believed on reasonable grounds to be engaged in terrorism (unless the applicant satisfied the Minister that their admission would not be detrimental to the national interest).

The Court found that the adjudicator departed from the definition of terrorism in *Suresh*, so the decision could not stand. The Court emphasized the need to identify specifically the acts of terrorism. It noted the definitions of "terrorist act" and "terrorist group" in the *Anti-terrorist Act*, but focused instead on the *Suresh* definition.

In *Sogi* v. *Canada (Minister of Citizenship and Immigration)*,[60] the applicant had been held inadmissible under IRPA section 34(1)(f), based on classified

---

58 [2003] FCJ No 540 (QL).

59 Replaced by similar provisions in section 34 of the *Immigration and Refugee Protection Act (IRPA),* SC 2001, c.27*:* a permanent resident or foreign national is inadmissible on security grounds for being a member of an organization believed on reasonable grounds to engage, has engaged or will engage in acts of espionage, subversion or terrorism.

60 [2003] FCJ No 1836 (QL).

information provided at an *in camera*, *ex parte* hearing that was not disclosed to the applicant. The application for judicial review was dismissed. The Court concluded the process did not infringe principles of fundamental justice. While noting it had no significance to the case, the Court pointed out that the groups the applicant was alleged to belong to had been listed under the *Anti-terrorism Act* as entities believed to engage in or to assist others in terrorist activities.

In *Alemu v. Canada (Minister of Citizenship and Immigration)*,[61] a visa officer had found that the applicant was neither a Convention refugee nor a member of the humanitarian designated class, and that there were reasonable grounds to believe the applicant was a person described in IRPA section 34(1)(f). Before the judicial review application, the Minister applied under IRPA section 87 for non-disclosure of information relied on by the visa officer, on the grounds that disclosure would be injurious to "national security or to the safety of any person". The Court granted the application, so the information was not disclosed to the applicant, counsel, or the public.

The Court held that the visa officer's conclusion that the applicant was a person under section 34(1)(f) was patently unreasonable. There were no specifically identified acts of espionage, subversion or terrorism by the organization to which the applicant was alleged to belong. The Court emphasized the need to use the *Suresh* definition in making determinations regarding terrorism, and noted further guidance found in the *Anti-terrorism Act*.

In *Ali v. Canada (Minister of Citizenship and Immigration)*,[62] an immigration officer refused to process an application for permanent residence as a Convention refugee, in light of IRPA section 34(1)(f). It was impossible to determine how the officer defined the term, so there was no adequate basis for the finding that the group with which the applicant was involved engaged in terrorist activities.

61 [2004] FCJ No 1210 (QL).

62 [2004] FCJ No 1416 (QL).

While the Court said that reference could be made to the definitions in the *Anti-terrorism Act*, its focus was again on the definition of terrorism in *Suresh*.

Security Certificates

Suspected terrorists who are not Canadian citizens are more likely to be the subject of a security certificate under IRPA, not charged with a terrorism offence under the *Anti-terrorism Act*. A Federal Court review of a security certificate issued under IRPA cannot be appealed.[63] Federal Court judges can draw different conclusions on the law, leaving the law in a state of uncertainty with no possibility of the differences being sorted out by the Federal Court of Appeal.

RECOMMENDATION

The CBA recommends that IRPA section 80(2) be amended to allow an appeal from a Federal Court decision on the reasonableness of a security certificate, with leave of the Federal Court of Appeal.

In a Federal Court review of a security certificate, the government can apply for non-disclosure to the person concerned where disclosure would be injurious to national security or to the safety of any person, examination of the information in private, and a hearing in the absence of person concerned.[64]

A person subject to a security certificate procedure should be allowed to submit specific questions on the Minister's summary of information. If the Minister objects to answering the question, the Court could rule on the objection. This procedure was followed in at least one case,[65] and should be formalized.

63 *IRPA*, section 80(2).

64 *IRPA*, section 78(a)(d) and (e).

65 In *re Harkat*, [2003] FC 918 at para 17, Dawson, J.

RECOMMENDATION

> **The CBA recommends that, where the Federal Court orders non-disclosure pursuant to IRPA section 78, the Court should appoint an *amicus curiae* to whom confidential material would be disclosed and who could represent the interests of the person concerned.**

A person detained for non-security reasons is entitled to a detention review after 48 hours, after seven days, and then every 30 days.[66] A person detained for security reasons is entitled to a detention review after 48 hours and then every six months.[67]

To some extent, this difference is mitigated by the fact that detention reviews in non-security cases can be waived by the detainee where there is no change of circumstances, and those detained for security reasons can apply for an accelerated detention review where there is a change of circumstances. However, we see no justification for the difference in the time lags for detention reviews for those detained for security and non-security reasons.

In *A (FC) and others (FC) v. Secretary of State for the Home Department,* [68] the U.K. House of Lords held that a detention scheme for suspected international terrorists different from that for other non-nationals subject to deportation violated the *European Convention on Human Rights* prohibition against discrimination. While the U.K. detention scheme for suspected international terrorists is different from the detention scheme for those subject to security certificates under IRPA, the decision nonetheless suggests a legal vulnerability of detention schemes for security risks that vary from detention schemes for other removal proceedings.

---

66 *IRPA*, section 57.

67 *IRPA*, section 83.

68 [2004] UKHL 56.

In *Hamdi v. Rumsfeld*,[69] the U.S. government sought to justify the detention of the person as an enemy combatant solely on the basis of evidence in a government declaration that, if believed, would justify the detention. The U.S. Supreme Court rejected that standard as a violation of due process under the U.S. Constitution. While Hamdi was a U.S. national and not subject to immigration removal proceedings, and the U.S. detention scheme was more draconian than the detention provisions in *IRPA* for those subject to security procedures, the case is a reminder that courts will enforce due process rights even in security cases.

RECOMMENDATION

The CBA recommends that those detained for security reasons be entitled to a detention review after 48 hours, after seven days and then every 30 days.

The *Immigration and Refugee Protection Regulations* should allow for deferral of removal of terrorists pending investigation for possible prosecution. The Regulations should grant the Minister of Citizenship and Immigration the power to stay enforcement of a removal order pending an investigation by the Attorney General into charges of participating in, facilitating, instructing or harbouring terrorist activity under the *Anti-terrorist Act*.

In some instances, persons subject to a security certificate are not removable from Canada because they would face torture or arbitrary execution. The government should adopt a policy of prosecuting these persons in Canada rather than incarcerating them indefinitely pursuant to the security certificate.

69 *Supra* note 29.

VII. TERRORIST FINANCING

Compelling Third Parties to Provide Information

Offences relating to terrorist financing (*Criminal Code* sections 83.02, 83.03 and 83.04) are broad and uncertain in scope, using phrases such as "directly or indirectly", "in whole or in part", "facilitating", and "benefiting". For example, it is an offence to "indirectly provide related services which will be used, in part, for the purpose of benefiting a person who is facilitating any terrorist activity" or to "indirectly use property, in part, for the purpose of facilitating terrorist activity". Criminal law must be certain, to limit the discretion of law enforcement.[70] Ambiguity allows the possibility of improperly exercised discretion to target people.

Monitoring and reporting requirements related to these offences are extraordinary in Canadian law, compelling non-state actors to participate in criminal investigations and information gathering strategies. This represents a fundamental shift in the approach to law enforcement in Canada. For example, section 83.11 requires financial institutions to "determine on a continuing basis whether they are in possession or control of property owned or controlled by or on behalf of a listed entity". Given the risk of prosecution and imprisonment, banks and loan companies faced with ambiguity will err on the side of over reporting, with the result that otherwise private information will be transmitted to a government agency where it may be further disseminated. With obvious difficulties in determining whether property is owned or controlled by or on behalf of a listed entity, there is plenty of room for ambiguity.

70 *Supra* note 11.

The *Proceeds of Crime (Money Laundering)* and *Terrorist Financing Act* imposes record keeping and reporting requirements to facilitate the investigation and prosecution of money laundering and terrorist financing offences. Section 7 requires a report to FINTRAC of every financial transaction "of which there are reasonable grounds to suspect that the transaction is related to the commission of a money laundering offence or a terrorist activity financing offence." Section 8 prohibits disclosure of the fact that a report has been made.

Again, non-state actors are compelled to provide information against third parties. Again, the third parties will not know that a report has been made, and will have no way to correct incomplete, misleading or false information, or to have the report deleted from government records.

Solicitor-client privilege is a fundamental tenet of the rule of law; people must be able to obtain independent legal advice without fear that their lawyer will disclose the nature of their inquiry to government authorities. The *Proceeds of Crime Act* initially required lawyers to report their clients to FINTRAC based on a suspicion of money laundering. Further, lawyers would not be able to tell their clients that they had made a report. These provisions were successfully challenged in court.[71]

RECOMMENDATION

The CBA recommends that *Criminal Code* section 83.1 be amended by adding an exception for information subject to solicitor-client confidentiality and privilege.

71 See, *The Law Society of BC v. AG Canada*, [2002] BCCA 49 (docket CA 029189/CA029190. The Federation of Law Societies and the Law Society of British Columbia launched a constitutional challenge of the money laundering legislation, in which the CBA intervened. In November 2001, the BCSC granted an interlocutory order exempting lawyers from the reporting scheme until the matter was finally determined, and in January 2002, the BCCA dismissed the Crown's appeal of the interlocutory order. Courts in other provinces then followed suit, and in March 2003, the federal government decided to exclude lawyers from the reporting scheme, but to reintroduce new rules in future, after consultation with the legal profession. The BC Supreme Court was scheduled to hear the challenge in November 2004, but all parties consented to a one-year extension.

VIII. IMPACT ON CHARITIES

Under the *Anti-Terrorism Act,* charitable activities thought until recently to be commonplace and uneventful may now make an innocent charity susceptible to:

- criminal charges for facilitating "terrorist activities" or supporting "terrorist groups."
- de-registration for suspected involvement in "terrorist activities", with the charity losing its charitable status and its directors exposed to personal liability.
- surveillance of its financial activities, potentially leading to allegations of terrorist financing.

However, the greatest impact of the *Anti-terrorism Act* may not be its direct application, but rather its indirect impact in creating fear of the "shadow of the law", even if the Act is never enforced against a charity.

De-Registration Process

The de-registration process lacks procedural safeguards and infringes principles of natural justice and due process:

- No knowledge or intent is required;
- The law is retroactive – past actions can be considered, as well as present and future;
- Normal rules for admissibility of evidence do not apply;
- The certificate is based on the low standard of "reasonable belief";
- "Confidential" information may not be disclosed to the charity, handicapping the charity's ability to present a full defence;
- The burden of proof shifts, requiring the charity to prove its innocence, even where it may not know the case against it;
- Due diligence by the charity is not a defence;
- No warning is issued or opportunity given to the charity to change its practices; and
- There is no legislated appeal or review by any court.

These factors have even more serious consequence with the issuance of a security certificate, which could lead to the charity's assets being the frozen or seized under sections 83.08 or 83.13-83.14 of the *Criminal Code*. The charity could be forced into bankruptcy, insolvency or winding up, exposing the charity's directors to civil liability for breach of their fiduciary duties by not adequately protecting the assets of the charity.

Discrimination

Political, religious and ideological purposes may be inherently suspect under the *Anti-terrorism Act* because they meet in part the definition of "terrorist activity".[72] Religious, ethnic and environmental charities may be scrutinized more than others, possibly resulting in discrimination against charities that have "religious or ideological" purposes.

Chill Effect on Charitable Activities

The legislation could have a chill effect on charitable activities by religious and humanitarian NGO's working in other countries. Organizations may be reluctant engage in overseas operations, humanitarian or otherwise, that could lead to loss of charitable status or *Criminal Code* violations. Due diligence to avoid situations that might attract liability are costly, difficult, and often ineffective, using resources that could be used for the charitable or humanitarian work. Actions by an agent of the charity involved in international operations could expose the charity and its directors to liability without their knowledge or intent.

In determining whether to accept a donation, charities must now look not only at the donor and its funds, but the means by which the donor raised funds. Donors may be reluctant to make donations that would result in the scrutiny of their financial affairs.

72 *Criminal Code* s. 83.01(1)(b)(i)(A), definition of terrorist activity.

International Developments Impacting Charities

Charities, NGOs and not-for-profit organizations are often identified as a "crucial weak point" in anti-money laundering and terrorist financing in the international community. The CBA acknowledges the potential problem and condemns any mechanisms that enable charities to finance terrorism. However, it is troubling that governments promote this view, when the Financial Action Task Force on Money Laundering (FATF) (of which Canada is a member) reports:

> The monitoring activities of supervisory or tax authorities responsible for NPO oversight do not appear to have identified any initial leads into terrorist financing cases within the charitable sector. However, these authorities have sometimes played an important role in developing relevant leads by being able to ask further questions or inspect entities and/or share information with law enforcement agencies. ."[73]

The Financial Action Task Force (FATF) (of which Canada is a member) has published the Eight Special Recommendations on Terrorist Financing and International Best Practices for Combating the Abuse of Non-Profit Organizations. The U.S. Treasury has issued Anti-terrorism Financing Guidelines: Voluntary Best Practices for U.S. Based Charities and a policy document 2003 National Money Laundering Strategy. The U.S. Agency for International Development (USAID) has expanded its mandate so that organizations receiving grants from the U.S. government will be considered "an arm of the U.S. government." This policy shift impairs the ability of NGOs to freely and impartially carry out humanitarian aid operations and to voice dissent about U.S. national security and foreign policy issues.

RECOMMENDATION

The CBA recommends that the federal government adopt "made-in-Canada" best practice guidelines, outlining requirements for charities to comply with the *Anti-terrorism Act*. The guidelines should be developed in consultation with

---

73 Financial Action Task Force on Money Laundering, "Report on Money Laundering Typologies 2003-2004" at para 42. http://www.fatf-gafi.org/dataoecd/19/11/33624379.PDF

representatives of the charitable sector, through the Charities Advisory Committee of the Canada Revenue Agency or another similar body.

International Emergencies and Disasters

When Parliament considered Bill C-36, many commentators argued against requiring aid agencies to determine the politics of groups they work with to get aid to the needy in times of emergency and disaster. Humanitarian assistance should not deny food, clothing and medical supplies to survivors, even terrorists, because of their political or religious beliefs.

Section 83.03 of the *Criminal Code* had the perverse result of potentially criminalizing the compassion of Canadians as they responded to the tsunami in South Asia with charitable dollars for relief and reconstruction work. The irony is that the federal government aided this conduct by matching funds. Some of the funds "benefit" organizations like the Liberation Tigers of Tamil Eelam, which qualifies as a "terrorist group". It controls the northern and eastern areas of Sri Lanka devastated by the tsunami. The government of Sri Lanka is at war with the Tamil Tigers and has no access to territory they control; the Tamil Rehabilitation Organization has the infrastructure to distribute the necessary relief supplies. Indeed, Prime Minister Martin sought permission from the government of Sri Lanka to visit the Tamil controlled area (which was denied) to see Canadian donations reached these victims of the tsunami. Other terrorist organizations fight for political independence from Indonesia in Aceh province in Sumatra. We question how Canadian charities and donors can know how to apply the law when the federal government has demonstrated that effective emergency relief can only be accomplished by ignoring the law.

RECOMMENDATION

The CBA recommends that the terrorism financing offences in the *Criminal Code* be amended to exempt registered charities

that provide funding or assistance for relief or humanitarian projects and programs that the federal government funds, supports, assists or gives aid to, either directly or indirectly, in response to international emergencies or disasters.

Public Perception

Associating charities in general with terrorist financing could have an ongoing negative impact on the general public perception of charities, making it more difficult to pursue charitable objectives:

- People may be less open to give to charitable operations, especially ones they are unfamiliar with, when a donation might expose them to criminal charges for facilitating terrorist activities.
- Donors may hesitate to give large donations that could expose their financial activities to government scrutiny under the *Proceeds of Crime Act*.
- Donors may hesitate to donate if there is a possibility the donation might not go to their intended purpose if the charity's assets are seized.

Liability Issues

Directors are accountable for their common law fiduciary duties for charitable property. Directors could be personally liable if the charity contravenes the *Anti-terrorism Act* and unnecessarily exposed the property of a charity to government seizure. Insurance coverage for directors and officers normally excludes fines, penalties and *Criminal Code* charges.

IX. RACIAL PROFILING AND HATE CRIMES

In Canadian jurisprudence, racial profiling has been defined as:

> "…criminal profiling based on race…(which) refers to that phenomenon whereby certain criminal activity is attributed to an identified group in society on the basis of race or colour resulting in the targeting of individual members of that group …[and] is illegitimately used as a proxy for the criminality or general criminal propensity of an entire racial group".[74]

74 *R.* v. *Richards* (1999), 26 CR (5th) 286 (Ont CA) (Rosenberg, J.A).

In addressing terrorism, racial profiling can be defined as a practice that:

> …involves separating a subsection of the population from the larger whole on the basis of specific criteria that purportedly correlates to risk, and subjecting the subgroup to special scrutiny for the purposes of preventing violence, crime or some other undesirable activity. Racial profiling thus entails the use of race as a proxy for risk either in whole or in part.[75]

Under *Criminal Code* section 83.3, law enforcement authorities, including immigration officials, may detain individuals on the basis of a reasonable ground to suspect that they are involved in terrorist activities or associated with terrorists. It is not surprising that the *Anti-terrorism Act* and other new legislation and policies have had an immediate impact on particular groups. The practice of issuing security certificates under the *Immigration and Refugee Protection Act*, for example, results in individuals being held indefinitely without bail, based on secret evidence that renders them unable to defend themselves and challenge their accusers.

Certainly, instances of racial profiling occurred before September 11. However,

> September 11 forced a fundamental shift in the racial profiling discourse. The central contention was no longer whether racial profiling was in fact taking place or how to best prevent incidents of racial profiling or even whether the Charter offered adequate remedial measures to address racial profiling. Rather, racial profiling debates in the context of the war against terrorism focus on whether Canadian society can morally, legally or politically condone racial profiling.[76]

Consequently, racial profiling has emerged as a tool to support Canadian's sense of security.

> Terrorism supplements all other lesser threats with a slightly different perspective that focuses more on the nature of the border and the symbolic and/or real reasons for maintaining one's border. The terrorist enemy has become the dangerous foreigner in our midst, with the policing task being to identify, remove, and incapacitate these persons.[77]

---

75 Bahdi, R., "No exit: racial profiling and Canada's war against terrorism" (2003) [unpublished, copy on file with author].

76 *Ibid*.

77 Beare, M., "Policing with a national security agenda" (Draft paper presented to the National Symposium on Policing in a Multicultural Society, February 2003) [unpublished].

RECOMMENDATION

The CBA recommends that federal, provincial, territorial and local governments adopt legislation, bylaws, policies, regulations and procedures to define racial profiling and take concrete measures to document, sanction and prohibit it.

At the same time, there has been a reported increase in hate activities directed at Arabs and Muslims, or those perceived to be Arabs and Muslims, across North America. The Canadian Muslim Civil Liberties Association has recorded 110 such incidents and the Canadian Islamic Congress indicates that such acts have increased by 1600% since September 11, 2001.[78]

The Jewish community has also been targeted. In 2004, crimes included the firebombing of a school library in Montreal, vandalism against synagogues in Toronto and St. John's and schools in Toronto and Ottawa, overturning tombstones in four Jewish cemeteries, and defacement of homes, cars, signs and other property in the Greater Toronto Area. A Toronto Police Service report shows that reported incidents of hate crimes in Toronto increased by nine per cent in 2004, with the Jewish community the single most targeted group.[79]

RECOMMENDATION

The CBA recommends that hate crimes be vigorously investigated and prosecuted.

78 *Supra* note 72 at 21,23.

79 Toronto Police Service, "2004 Annual Hate/Bias Crime Statistical Report", online: <http://www.torontopolice.on.ca/publications/files/reports/2004hatecrimereport.pdf>.

X. PRIVACY AND PROTECTION OF PERSONAL INFORMATION

Privacy is protected through the right to be secure against unreasonable search or seizure, and is fundamental to security of the person. State collection of personal information has profound implications for privacy interests.

The Supreme Court of Canada has attached importance to the protection of privacy in a number of judgments. In *R. v. Duarte*, the Court observed "one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance."[80] In *R. v. Wong*, the Court held:

> …the broad and general right to be secure from unreasonable search and seizure guaranteed by s.8 is meant to keep pace with technological development, and, accordingly, to ensure we are ever protected against unauthorized intrusions upon our privacy by the agents of the state, whatever technical forms the means of invasion might take.[81]

In *R. v .Law*, the Court held that informational privacy "derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain … as he sees fit."[82]

The widespread use of technology and human sources to gather information, and the use of technology to collate and disseminate information makes the protection of private information critical to this review.[83]

Privacy, Access to Information and PIPEDA

Sections 87, 103 and 104 of the *Anti-terrorism Act* amended the *Access to Information Act*, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) respectively, to permit the Attorney General

80 *R. v. Duarte*, [1990] 1 SCR 30.

81 *R. v. Wong*, [1990] 3 SCR 36.

82 *R. v. Law*, [2002] 1 SCR 227.

83 See more detailed discussion regarding privacy, *infra* at 38-42.

of Canada to issue a certificate prohibiting disclosure of information to protect international relations or national defence or security. The Acts are inoperative for information covered by the certificate.

Information legitimately classified as sensitive that relates to compelling national interests should be protected. However, the CBA continues to have concerns about these provisions. The *Privacy Act* protects the privacy of personal information held by a government institution and gives individuals a right of access to that information. PIPEDA protects personal information gathered in the course of commercial activities and provides for complaints to the Privacy Commissioner. The *Access to Information Act* enables Canadians to obtain information about the operation of government. These statutes provide an important framework for the protection and regulation of personal and public information in the federal sphere. An independent commissioner oversees each statute. The protected interests go to the heart of individual autonomy and democratic participation in Canadian society. Any derogation from these interests requires careful balancing between individual and state interests, along with meaningful protections against abuses.

Canadians have a legitimate interest in obtaining information about government and its operations. Transparency permits meaningful public participation in the political process. Canadians also have an interest in ensuring that private, personal information is used only for legitimate purposes and is not disclosed to others. While governments and (with consent) businesses routinely collect personal information, the *Privacy Act* and PIPEDA ensure it is for reasonable purposes, in the least intrusive manner and in a manner that protects information from unauthorized disclosure.

Before the *Anti-terrorism Act* amendments, all three statutes prevented disclosure of information where there were compelling national security interests. Each required balancing of interests along with meaningful oversight. The *Anti-*

terrorism Act amendments tilted the balance against the interests originally served by the laws. Individuals are denied the rights otherwise accorded to them under ATIA, the *Privacy Act* and PIPEDA, to the extent that the information is listed in a certificate.

There is no right to independent review by the Privacy Commissioner, the Information Commissioner, or any other authority as a check on the unfettered powers of the Attorney General. There is no meaningful oversight in national security circumstances. A certificate need not be published under the *Statutory Instruments Act.* The Attorney General need not report to Parliament on the exercise of these powers. Certificates are issued in the shadows, inconsistent with open and fair government. Some form of review is appropriate, to ensure the power is not abused.

Before the *Anti-terrorism Act* amendments, the three statutes applied a "harms" test to disclosure of information on international relations, defence and national security. If disclosure was reasonably expected to be "injurious" to these interests, the information could be withheld. Sections 87, 103 and 104 contain no harm test, or any need to weigh public interests. They do not require the Attorney General to specify the information subject to the certificate.

The certificate should specifically identify the type, category or description of information in question, to enable both data holders (branches of government and businesses) and data subjects (individuals) to know what is involved and to assist in compliance. Certificates should contain a general account of the interest to be protected. In addition, the *Anti-terrorism Act* does not contain any means for the public to find out whether a certificate has been issued in relation to particular information. If sections 87, 103 and 104 are not repealed, then the *Anti-terrorism Act* should be amended to provide the above clarifications. This would provide more certainty and allow for public debate of the particular measures.

We have concerns about the Attorney General's power as it relates to portions of PIPEDA. PIPEDA already contains detailed provisions prohibiting disclosure of personal information, including for national security purposes (section 9). The *Anti-terrorism Act* should specify what data holders should do when they face competing disclosure obligations. Can data holders disclose information subject to a certificate in accordance with obligatory disclosure requirements in PIPEDA, under the exclusions contained in section 7(3) of PIPEDA or under other legislation?

The issuance of a certificate under this provision would potentially affect data holders' abilities to comply with PIPEDA in a number of ways. It removes substantive rights of data subjects explicitly granted under PIPEDA — for example the right to ensure accuracy of their personal information, the right to access their personal information, and their entitlement to independent review. Again, there is no statutory review mechanism for data holders or data subjects to challenge the validity of the certificate or its conditions.

The Act provides for no life span for the access-barring effect of the certificate and the CBA recommends that it should be no longer than five years, subject to any renewal if the conditions justifying the certificate still apply. The CBA also recommends, in the alternative, that Parliament impose "sunset clauses" on the above amendments to the Privacy Act, ATIA and PIPEDA so that they become inoperative within five years unless expressly extended by Parliament.

RECOMMENDATION

The CBA recommends that sections 87, 103 and 104 of the *Anti-terrorism Act* be repealed.

In the alternative, the CBA recommends that:

(a) specific criteria be stipulated for issuing a certificate;

(b) a statutory review procedure be established, which would not necessarily suspend the immediate operative effect of a certificate pending any decision being rendered;

(c) a more refined approach be considered, for instance enabling an individual to continue to access or challenge personal information;

(d) the certificate specify the type, category or description of information in question;

(e) the certificate be published pursuant to the *Statutory Instruments Act*;

(f) the certificate cease to have effect after five years; and

(g) the Attorney General be required to report annually the number of certificates and the general circumstances of each to Parliament.

Biometric Technology and National Identity Cards

In a 2003 submission responding to a proposal to introduce a national identity card, the CBA noted that a national identification system complete with biometric data was a controversial shift in policy and practice. The CBA recommended that the government clearly and fully disclose the purpose, capabilities, and use of a national identity card, to properly inform public debate. The CBA also recommended that, if a national identity card were to be introduced, it be limited to confirmation of identity and status, with or without biometric identifiers. There should be no imbedded information or accessible database until the privacy intrusion capacities are fully disclosed, and there has been clear and informed approval outlining the extent of acceptable privacy intrusion, and the circumstances under which disclosure will be mandatory and to whom. If a national identity card were introduced, the government should clearly delineate very limited circumstances requiring possession and presentation of the card, as well as a clear statement of consequences of not possessing and presenting it.

In summary, the CBA expressed strong concerns about a national identity card for Canadians because:

- It is unclear what the purpose and scope of the card would be.

- There are significant privacy concerns with the use of imbedded information and database information that could be accessed through a card.

- If the card were for permanent residents, it would duplicate the existing PR Card; if it were for citizens, there would be a marginal benefit at most, as many already possess satisfactory evidence of status through birth certificates and passports.

- If the card would be applicable to foreign nationals (students, workers, visitors and refugee claimants), then the PR Card experience puts in question whether the process would be cost effective, timely and capable of flexibility to adapt to the changing status of such individuals.

- Even if limited to a biometric secure identity card confirming status and standard identity data, the production costs and infrastructure involved may be overwhelming.

Technology is a tool to implement public policy, not a capability to drive policy.

XI. SUMMARY OF RECOMMENDATIONS

The Canadian Bar Association recommends that:

1. the federal government indicate clearly the adoption of Canada's obligations under international conventions and instruments in Canadian domestic law, and list in annual reports on the *Anti-terrorism Act* cases applying Canada's obligations under international conventions and instruments.

2. terrorist activities be defined consistently in all Canadian laws relating to terrorism, adopting the definition in the UN *Convention for the Suppression of the Financing of Terrorism*:

> Any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

3. the *Criminal Code* be amended to require the Crown to prove criminal intent to find anyone guilty of a terrorist offence.

4. lawyers providing legal services to those accused of terrorist offences be specifically excluded from the ambit of section 83.18, dealing participation in or contribution to an activity of a terrorist group.

5. *Criminal Code* section 25.1 and related sections be repealed, so that public officers are not legally justified in committing criminal offences.

6. the federal government:
    1. enact regulations with safeguards for sharing information with regimes that do not respect human rights, to ensure that the information is shared in a manner that does not put Canadian citizens at risk;
    2. share raw intelligence information with the caveat that the information has not been proven and that it should be acted on only with caution;
    3. affirm that it is unacceptable for Canadian citizens to be deported from other countries to undemocratic regimes or regimes that engage in torture, and insist that Canadian citizens instead be returned to Canada; and
    4. establish an independent compensation mechanism to which Canadian citizens suffering harm because of information shared without proper safeguards can apply for compensation.

7. the federal government establish an independent oversight mechanism for all security matters not covered by SIRC.

8. *Canada Evidence Act*:

    1. section 38 et seq. be amended to make public the fact of an application to the Court, and to ensure that proceedings are open to the public to the greatest extent possible taking security considerations into account.
    2. section 38.06 be amended to preclude the use of summaries of evidence in criminal proceedings.

9. IRPA section 80(2) be amended to allow an appeal from a Federal Court decision on the reasonableness of a security certificate, with leave of the Federal Court of Appeal.

10. where the Federal Court orders non-disclosure pursuant to IRPA section 78, the Court should appoint an *amicus curiae* to whom confidential material would be disclosed and who could represent the interests of the person concerned.

11. those detained for security reasons be entitled to a detention review after 48 hours, after seven days and then every 30 days.

12. *Criminal Code* section 83.1 be amended by adding an exception for information subject to solicitor-client confidentiality and privilege.

13. the federal government adopt "made-in-Canada" best practice guidelines, outlining requirements for charities to comply with the *Anti-terrorism Act*. The guidelines should be developed in consultation with representatives of the charitable sector, through the Charities Advisory Committee of the Canada Revenue Agency or another similar body.

14. the terrorism financing offences in the *Criminal Code* be amended to exempt registered charities that provide funding or assistance for relief or humanitarian projects and programs that the federal government funds, supports, assists or gives aid to, either directly or indirectly, in response to international emergencies or disasters.

15. federal, provincial, territorial and local governments adopt legislation, bylaws, policies, regulations and procedures to define racial profiling and take concrete measures to document, sanction and prohibit it.

16. hate crimes be vigorously investigated and prosecuted.

17. sections 87, 103 and 104 of the *Anti-terrorism Ac*t be repealed. In the alternative:

(a) specific criteria be stipulated for issuing a certificate;

(b) a statutory review procedure be established, which would not necessarily suspend the immediate operative effect of a certificate pending any decision being rendered;

(c) a more refined approach be considered, for instance enabling an individual to continue to access or challenge personal information;

(d) the certificate specify the type, category or description of information in question;

(e) the certificate be published pursuant to the Statutory Instruments Act;

(f) the certificate cease to have effect after five years; and

(g) the Attorney General be required to report annually the number of certificates and the general circumstances of each to Parliament.