

## Bill C-51, Anti-terrorism Act, 2015

### **CANADIAN BAR ASSOCIATION**

**March 2015** 

#### **PREFACE**

The Canadian Bar Association is a national association representing 36,000 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 Canadian Bar Association with contributions from the National Criminal Justice, Immigration Law, International Law, Aboriginal Law, Environmental, Energy and Resources Law, Charities and Not-for-Profit Law and the Privacy and Access to Information Law Sections, and 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.

## **TABLE OF CONTENTS**

## Bill C-51, Anti-terrorism Act, 2015

<b>EXEC</b>	UTIV	E SUMMARY	. 1		
	A.	Canadian Security Intelligence Service (CSIS)			
	B.	Information Sharing3			
	C.	Criminal Code amendments 4			
	D.	Coherent National Oversight5			
	E.	CONCLUSION5			
I.		RODUCTION – PROTECTING SAFETY AND SERTIES	. 7		
II.		REFUL CONSIDERATION, NOT CURSORY	. 9		
III.	INFORMATION SHARING THAT RESPECTS PRIVACY9				
	F.	Targeting Activity that Undermines the Security of Canada, not Legitimate Dissent			
	G.	Scope of Disclosure – Preserving Personal Privacy 12			
	Н.	Limited Checks and Balances14			
	I.	SCISA Needs Effective Review and Accountability 16			
IV.		CLARIFYING RESTRICTIONS IN SECURE AIR TRAVEL ACT17			
V.	MAKING BETTER USE OF THE CRIMINAL CODE 21				
	A.	What it means to "Advocate or Promote" Terrorism			
	B.	Properly Targeting Terrorist Propaganda25			
	C.	Preventive Detention is an Extraordinary Measure26			
	D.	Use Peace Bonds Instead of Control Orders28			

VI.	MONITORING NATIONAL SECURITY, INCLUDING CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS)				
	<b>(Ο.</b> Α.	Kinetic powers require oversight			
	В.	Judges should not authorize Charter Violations			
	С.	CSIS should be bound by the Charter			
	D.	Need for Oversight and Review			
	Б. Е.	Robust Reporting means Better Protection			
	F.	Parliamentary Review of Law			
VII.	MAKING BETTER USE OF THE IMMIGRATION AND REFUGEE PROTECTION ACT37				
	A.	Ensuring Effectiveness of Special Advocates	37		
	B.	Fair Appeals for All Parties	40		
		Lifting the leave requirement  Lifting the "certified question" requirement			
VIII.	PROTECTING THE WORK OF CHARITIES AND NOT-FOR-PROFITS41				
	A.	Security of Canada Information Sharing Act	42		
	B.	Secure Air Travel Act			
	C.	New Terrorism Offence	43		
IX.	CC	NCLUSION	44		
Χ.	SU	MMARY OF RECOMMENDATIONS	45		

## Bill C-51, Anti-terrorism Act, 2015

### **EXECUTIVE SUMMARY**

The 2001 *Anti-terrorism Act* signaled a fundamental shift in Canada's approach to combatting terrorist acts, with significant changes to Canadian law to address those threats. After more than a decade of experience since the *Anti-terrorism Act* became law, some of its provisions have proven useful, while others have not. As the CBA and many others predicted in 2001, this experience has left little doubt about the discriminatory impact of anti-terrorism laws on some populations.

The CBA acknowledges that Canadians are concerned about terrorism – at home or abroad – and supports the government's intention to reduce the risk of terrorist acts in Canada. The CBA supports measures to improve public safety that are necessary, proportionate and accompanied by adequate safeguards against abuse. The government must show Canadians that the further powers in Bill C-51 meet this standard.

The government should also be clear with Canadians about the limits of law. No law, no matter how well-crafted or comprehensive, can prevent all terrorist acts from occurring. Promising public safety as an exchange for sacrificing individual liberties and democratic safeguards is not, in our view, justifiable. Nor is it realistic. Both are essential and complementary in a free and democratic society.

The key question is, "Does the bill strike the appropriate balance between enhancing state powers to manage risk and safeguarding citizens' privacy rights and personal freedoms?"

Our comments and legal analysis are offered to assist Parliament to improve the Bill, and we would be happy to provide further assistance on any specific issue. The CBA's full submission provides a detailed analysis of all parts of the Bill. This Executive Summary focuses on three parts of the Bill, and one overarching concern:

 CSIS Act changes that would conscript judges to authorize Charter violations and unlawful acts, under the guise of providing judicial oversight

- Creating the *Security of Canada Information Sharing Act (SCISA)*, to significantly expand information sharing powers without adequate definition and clarity, and without basic concepts of privacy protection
- New criminal law powers and offences that are vague and too broad, making them vulnerable to constitutional challenge, and likely to impact legitimate political dissent
- The absence of coherent expanded national oversight to balance significant proposed new state powers.

## A. Canadian Security Intelligence Service (CSIS)

Bill C-51 would transform CSIS from an intelligence-gathering agency to an agency actively engaged in countering national security threats. It would allow CSIS to employ undefined "measures" "within or outside of Canada" to "reduce" a "threat to the security of Canada". The threshold for using those measures would be "reasonable grounds to believe a particular activity constitutes a threat to the security of Canada".

The powers of CSIS have always depended on how a "threat to the security of Canada" is defined, and section 2 of the *CSIS Act* already has an extremely broad definition. This has been interpreted to include environmental activists, indigenous groups, and other social or political activists. Concerns are heightened with the proposal to grant CSIS a "disruptive" kinetic role.

The limits in the Bill are not enough. The decision as to what constitutes "reasonable and proportional" will fall unilaterally to those within government and CSIS. A warrant under section 21.1 is required *only* if CSIS has "reasonable grounds" to believe that it is required, and only where the measures "will" (not "may") contravene a *Charter* right or a Canadian law. Measures short of what CSIS determines to be a certain *Charter* violations or criminal act require no warrant.

The combination of the proposed section 12.1(3) and the warrant provisions in section 21.1 appear to provide for judicial warrants to authorize not only contraventions of the criminal law and *Charter* rights, but the violation of *any Charter* rights – making the entire *Charter* at risk. This is unprecedented.

Judicial warrants for search and seizure *prevent*, not *authorize*, *Charter* violations. A judge authorizing a search is not authorizing a breach of the *Charter*, but may authorize a search to prevent what would otherwise be a breach of section 8. Other *Charter* rights, such as the

right against cruel and unusual punishment or mobility rights, are absolute, and their violation can never be "reasonable".

It is untenable that the infringement of Charter rights is open to debate, in secret proceedings where only the government is represented. Parliament should not empower CSIS or judges to disregard the constitutional foundations of our legal system.

## **B.** Information Sharing

Bill C-51 would establish the *Security of Canada Information Sharing Act (SCISA)* creating authority for federal government institutions to share information – including personal information – about "activities that undermine the security of Canada". Targeted activities are defined broadly, based on whether they undermine the "sovereignty, security or territorial integrity of Canada" or the "lives or the security of the people of Canada".

What will constitute threats to the "security of Canada" includes activities that interfere with the "economic or financial stability of Canada". Canadians have seen this language applied broadly, for example to instances of labour unrest, Aboriginal protest and environmental activism. The exception for "lawful advocacy, protest, dissent and artistic expression" is too narrow. Legitimate advocacy and protest that is both important and common in a democratic society can often be unlawful due to breach of regulatory rules or municipal bylaws.

There are insufficient checks and balances in *SCISA*, and no safeguards to ensure that shared information is reliable. Maher Arar's experience illustrated the devastating consequences of sharing inaccurate or unreliable information. The broad scope of disclosure under sections 5 and 6 is also a concern. While *SCISA* is theoretically subordinate to the *Privacy Act*, <sup>1</sup> the latter explicitly allows disclosure as authorized by *any* other *Act of Parliament*, <sup>2</sup> so would in turn permit any disclosure under the proposed *SCISA* that might otherwise be prohibited.

Additional clarification of key terms and due consideration of those basic concepts is needed, along with sufficient information sharing controls and effective oversight. The CBA also recommends Parliamentary review of the act at regular intervals.

<sup>&</sup>lt;sup>1</sup> SCISA, section 5(1),

<sup>&</sup>lt;sup>2</sup> *Privacy Act*, RSC 1985, c P-21, section 8(2)(b).

## C. Criminal Code amendments

A primary principle of criminal law is that people know in advance what conduct is prohibited and what is not. Bill C-51 proposes several *Criminal Code* amendments that generally suffer from overly broad language, uncertainty and vagueness. These weaknesses would make the proposals vulnerable to constitutional challenge and have little, if any, impact on public safety.

Advocating or promoting terrorism (section 83.221) would apply to all "statements", apparently including private statements, emails and text messages. The reference to "terrorism offences in general" seems to indicate an intent to cast the net broadly and loosely, to include existing terrorism offences and other indictable offence committed for the benefit of, at the direction of, or in association with a terrorist group. Criminal acts can best be detected and prevented by allocating sufficient resources to law enforcement. If narrowly construed by the courts, the proposal will add nothing to existing offences such as counselling the commission of an offence, advocating genocide, or contributing to a terrorist organization. If widely construed, it will be subject to significant challenges, at great cost to taxpayers, and may include activity more political in nature than dangerous.

"Terrorist propaganda" (section 83.222) would authorize deletion of "terrorist propaganda", defined as "any writing, sign, visible representation or audio recording that advocates or promotes the commission of terrorism offences in general ... or counsels the commission of a terrorism offence". We support in principle deletion orders for "terrorist propaganda", but this net is cast too wide. There is no requirement of mental fault and the proposal lacks public interest, education, or religious discussion defences. "Terrorist propaganda" should be confined to material that counsels the commission of a terrorist offence or that instructs the commission of a terrorist offence.

**Preventive detention** aims to avert imminent and serious terrorist threats where there is no evidence to support reasonable and probable cause for arrest and charge for a criminal offence. Bill C-51 would reduce the legal thresholds required, extend the permissible period of detention and omit a sunset clause. It would make permanent what was once justified as a temporary and exceptional legal measure, and make this extraordinary legal measure more robust, all without evidence to show that the existing law has been useful or changes are warranted.

**Peace bonds and control orders** would rely on a significantly lower standard than currently exists. A peace bond is now available if a person fears, on reasonable grounds, that another person *will* commit a terrorism offence. Under Bill C-51 the threshold would be whether someone *may* commit a terrorism offence. The CBA supports this reduced standard as an effective way to ensure the timely disruption of possible terrorist threats. The maximum duration of a peace bond would increase from two years to five years if the defendant was previously convicted of a terrorism offence. The increase may lead the section to be susceptible to constitutional challenge and prolong and complicate criminal proceedings as courts struggle to determine if a previous conviction was for a "terrorism offence" (given vagueness of the definition of "terrorism"). Section 810.01(1) already addresses terrorism offences and could be amended to more effectively manage risks of terrorism, so the proposal for new control orders is redundant.

## **D. Coherent National Oversight**

Many Arar Commission and Air India Commission recommendations surround shortcomings of the current oversight and review regimes. Those recommendations have yet to be implemented. **Expanding national security powers without a corresponding reinforcement and expansion of an insufficient oversight and review is a serious problem.** An expert review body must be created with resources and a mandate to review *all* national security activity. The CBA also recommends Parliamentary review by a committee with access to secret information.

## E. CONCLUSION

The CBA supports government efforts to enhance the safety and security of Canadians that are necessary, proportionate and accompanied by adequate safeguards against abuse. Promising public safety as an exchange for sacrificing individual liberties and democratic safeguards is not, in our view, justifiable or realistic. Both are essential and complementary in a free and democratic society. Safety cannot be won at the expense of Canada's constitutional rights and freedoms.

When extraordinary powers of surveillance, intelligence-gathering and sharing, preventive arrest and detention are contemplated, shown to be necessary and then implemented, equally extraordinary mechanisms of oversight and after-the-fact review must also be in place to provide the necessary balance to those initiatives.

For Bill C-51 to be a meaningful success, Canadians must not only feel safer but must in fact be safer – and this reality must be accompanied by the well founded and secure belief that Canada remains a democracy that leads the way internationally in scrupulously protecting privacy rights and civil liberties.

## Bill C-51, Anti-terrorism Act, 2015

# I. INTRODUCTION – PROTECTING SAFETY AND LIBERTIES

The Canadian Bar Association (CBA) acknowledges that Canadians are concerned about terrorism –at home or abroad – and supports the government's intention to reduce the risk of terrorist acts in Canada. Our comments and legal analysis are offered to assist Parliament to improve the Bill, and we would be happy to provide further assistance on any specific issue.

The key question is, "Does the bill strike the appropriate balance between enhancing state powers to manage risk and safeguarding citizens' privacy rights and personal freedoms?" While the CBA supports the objectives of Bill C-51, many of the measures proposed do not strike the appropriate balance. The analysis that follows emphasizes the CBA concerns about:

- the conscription of judges to authorize *Charter* violations and unlawful acts by CSIS, contrary to judges' fundamental role in upholding Canada's constitution and the Rule of Law
- how aspects of the Bill will withstand constitutional scrutiny
- lack of precision and overly broad language of key provisions of the Bill
- how fundamental concepts of criminal law can be reconciled with new proposed offences
- the absence of expanded national oversight to balance proposed new state powers.

The 2001 *Anti-terrorism Act* signaled a fundamental shift in Canada's approach to combatting terrorist acts, with significant changes to Canadian law to address those threats. At the time, many organizations, including the CBA questioned whether the new law was necessary, that is, whether adequate tools already existed in Canadian criminal law to combat terrorism. The CBA has previously cautioned that:

If these sections become an accepted part of the normal fabric of criminal law, the original exceptional justification for the provisions may well be forgotten. The general explanation that they make law enforcement more effective could easily be used to justify extending them beyond their present limits.<sup>1</sup>

After more than a decade of experience since the *Anti-terrorism Act* became law, some of its provisions have proven useful, while others have not. Some of the limits to state action against individuals have been respected, and in other cases, those limits have been lacking. As the CBA and many others predicted in 2001, this experience has left little doubt about the discriminatory impact of anti-terrorism laws on some populations.<sup>2</sup>

The CBA supports measures to improve public safety that are necessary, proportionate and accompanied by adequate safeguards against abuse. The onus is on government to show Canadians with solid fact-based evidence that the further powers in Bill C-51 meet this standard. The government should also be clear with Canadians about the limits of law. No law, no matter how well-crafted or comprehensive, can prevent all terrorist acts from occurring.

Promising public safety as an exchange for sacrificing individual liberties and democratic safeguards is not, in our view, justifiable. Nor is it realistic. Both are essential and complementary in a free and democratic society. As former Supreme Court Justice Ian Binnie said:<sup>3</sup>

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.

The CBA acknowledges and commends the analysis of Professors Kent Roach of the University of Toronto and Craig Forcese of the University of Ottawa on various aspects of Bill C-51.4

Letter re: Bill S-7, Combating Terrorism Act (Ottawa: CBA, 2012).

For just one example, see <a href="www.cbc.ca/news/innocent-traveller-stuck-on-airline-watch-list-1.984446">www.cbc.ca/news/innocent-traveller-stuck-on-airline-watch-list-1.984446</a>.

Justice Binnie, *Application under section 83.28 of the Criminal Code (Re)*, [2004] 2 SCR 248, para. 116.

<sup>4</sup> See <u>www.antiterrorlaw.ca</u>.

## II. CAREFUL CONSIDERATION, NOT CURSORY STUDY

The Public Safety and National Security Committee has limited its study of Bill C-51 to eight hearings involving 48 witnesses, mainly occurring in the week of March 23, with clause-by-clause review on March 31, 2015. The importance of the proposed legislation is difficult to overstate, and the CBA believes that this process is too rushed given the interests at stake. Bill C-51 deserves careful review and debate, with consideration of the perspectives of all relevant organizations and individuals with expertise in this area.

### III. INFORMATION SHARING THAT RESPECTS PRIVACY

Part I of Bill C-51 would establish the new *Security of Canada Information Sharing Act* (*SCISA*). *SCISA* would authorize federal government institutions to share information (presumably including personal information) about "activities that undermine the security of Canada" (targeted activities) with other specified federal government institutions. Targeted activities are defined in section 2, and would include the following, if they undermine the "sovereignty, security or territorial integrity of Canada" or the "lives or the security of the people of Canada":

- (a) interference with the capability of the Government of Canada in relation to intelligence, defence, border operations, public safety, the administration of justice, diplomatic or consular relations, or the economic or financial stability of Canada;
- (b) changing or unduly influencing a government in Canada by force or unlawful means;
- (c) espionage, sabotage or covert foreign-influenced activities;
- (d) terrorism;
- (e) proliferation of nuclear, chemical, radiological or biological weapons;
- (f) interference with critical infrastructure;
- (g) interference with the global information infrastructure, as defined in section 273.61 of the *National Defence Act*;
- (h) an activity that causes serious harm to a person or their property because of that person's association with Canada; and
- (i) an activity that takes place in Canada and undermines the security of another state.

The Preamble to *SCISA* states that "there is no more fundamental role for a government than protecting its country and its people".<sup>5</sup> The CBA emphasizes that there must be an appropriate balance between measures intended to improve public safety (including the legitimate government interest in sharing information about actual security threats between government agencies) and those designed to protect other fundamental aspects of Canadian democracy and constitutional values. In our view, the proposed *SCISA* would implicate activities that cannot be legitimately characterized as security threats.

Section 4 of *SCISA* proposes principles to guide information sharing:

- (a) Effective and responsible information sharing protects Canada and Canadians;
- (b) Respect for caveats on and originator control over shared information is consistent with effective and responsible information sharing;
- (c) Entry into information sharing arrangements is appropriate when Government of Canada institutions share information regularly;
- (d) The provision of feedback as to how shared information is used and as to whether it is useful in protecting against activities that undermine the security of Canada facilitates effective and responsible information sharing;
- (e) Only those within an institution who exercise its jurisdiction or carry out its responsibilities in respect of activities that undermine the security of Canada ought to receive information that is disclosed under the act.

The CBA supports these principles, and suggests that *SCISA* include a mechanism to enforce them.

#### **RECOMMENDATION:**

1. The CBA recommends that *SCISA* include effective mechanisms to enforce the principles outlined in section 4.

# F. Targeting Activity that Undermines the Security of Canada, not Legitimate Dissent

"Activity that undermines the security of Canada" is defined in section 2 of SCISA as "any activity ... if it undermines the sovereignty, security or territorial integrity of Canada or the

See, Canada (Public Safety and Emergency Preparedness) v. Agraira, 2011 FCA 103. The Federal Court of Appeal found that the statutory emphasis on "security" in the Department of Public Safety and Emergency Preparedness Act, SC 2005, c. 10, and related provisions in other acts, was meant to make security the principal and perhaps the dispositive consideration in decisions made by the Minister on certain immigration applications. This position was moderated, but not overturned, by the Supreme Court: Agraira v. Canada (Public Safety and Emergency Preparedness), [2013] 2 SCR 559, 2013 SCC 36.

lives or the security of the people of Canada". This definition is overly broad and without sufficient interpretative guidance. The result is a vast scope for information sharing in situations unrelated to the Bill's anti-terrorism objectives.

"Security of Canada" is not defined in *SCISA*. Under paragraph (a) of the activity definition in section 2, it would include activities that interfere with the capability of the government in relation to the "economic or financial stability of Canada." Canadians have already seen this language applied broadly, for example to instances of labour unrest, Aboriginal protest and environmental activism.<sup>6</sup> In cases such as *Suresh v. Canada (Minister of Citizenship and Immigration)*, the possibility was open that a person could cause a "danger to the security of Canada", not because of any blameworthy conduct, but because their actions anger a needed ally.<sup>7</sup> The "people of Canada" includes any Canadian, even if they are outside Canada. The words "activities" and "undermine" are not defined in the Act, leaving open a range of actions that may trigger information sharing powers.

The activity definition also lists examples of "activities that undermine the security of Canada" and "terrorism" is only one example. The list illustrates the scope of the proposed information sharing regime, and raises several important concerns:

- "Interference with the capability of the Government of Canada in relation to
  intelligence, defence, border operations, public safety, the administration of justice,
  diplomatic or consular relations, or the economic or financial stability of Canada" is too
  broad. In particular, the references to "public safety" and the "economic or financial
  stability of Canada" would authorize information sharing in cases of non-political crime
  and actions that do not relate to issues of Canadian security.
- The phrase "critical infrastructure" in item (f) is not defined. It would likely include pipelines and hydro transmission towers, and possibly blockades of railways and roadways. It could capture peaceful protestors who blockade a pipeline, in breach of regulatory rules or municipal bylaws. Again, information sharing would be authorized for activities that do not relate to national security and in fact are important and common for Canada's democracy.

For example, see "Anti-Petroleum Movement a Growing Threat to Security of Canada, RCMP says" (Feb 17 2015, Globe and Mail) <a href="https://www.theglobeandmail.com/news/politics/anti-petroleum-movement-a-growing-security-threat-to-canada-rcmp-say/article23019252/">www.theglobeandmail.com/news/politics/anti-petroleum-movement-a-growing-security-threat-to-canada-rcmp-say/article23019252/</a>

That case references international cooperation as necessary for the security of Canada, and says that danger to that security does not need to be direct. See, *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1 at paras. 87-92.

• Also unanswered is *what will constitute a determination that someone is "undermining the security of another state"* and how this will be applied in a way that is democratic, safe, and fair to all Canadians. It could, for example, capture public protests that affect the security of another state, if the protests are done without the proper permits so technically unlawful. This would be true even if the other state is a repressive one. Thus, APEC or Falun Gong protests might trigger the proposed information sharing provisions.

It is unclear how the breadth of these activities would advance Bill C-51's anti-terrorism objectives. Branding dissenting Canadian views as threats to the security of Canada is contrary to core democratic principles important to Canadians and risks a chilling impact on free expression in this country.

"Lawful advocacy, protest, dissent and artistic expression" is excluded from the activity definition in section 2, but this exception is too narrow. Advocacy and protest may be unlawful due to breach of regulatory rules or municipal bylaws. *SCISA* would authorize information sharing even in those cases, despite the fact that the advocacy or protest could not legitimately be characterized as a security threat. The exemption in section 2 should include unlawful protests that do not represent a genuine threat to national security, in keeping with the exemption for protests and strikes in the definition of "terrorist activity" in the *Criminal Code*.8

In a free and democratic society, civil disobedience and unlawful protests should not be treated as national security threats, unless they actually are life threatening.

#### **RECOMMENDATION:**

2. The CBA recommends the scope of activities subject to information sharing under *SCISA* be narrowed, and that the exemption in section 2 of *SCISA* be expanded to specifically include unlawful protests that do not represent a genuine threat to national security.

## G. Scope of Disclosure – Preserving Personal Privacy

The heart of *SCISA* is section 5, which states that upon request *or* on its own initiative, and in compliance with all other law, a Government of Canada institution may disclose

See section 83.01(b)(ii)(E) of the *Criminal Code of Canada*.

"information". This is not defined, but would presumably mean that information including personal information could be disclosed to the other Government of Canada institutions under certain circumstances. Section 6 seems to allow for "purpose creep" contrary to the *Privacy Act* and fundamental principles of privacy law, and would open the door to misuse of private information.

The term "government institution", under section 2, is as defined in the *Privacy Act*, or any institution listed in Schedule 2 of *SCISA*. Under the *Privacy Act*, "government institution" is:

- (a) any department or ministry of state of the Government of Canada, or anybody or office, listed in the schedule, and
- (b) any parent Crown corporation, and any wholly-owned subsidiary of such a corporation, within the meaning of section 83 of the *Financial Administration Act*.

Over 140 institutions are listed under the *Privacy Act*. Schedule 2 lists 17 government institutions, including CSIS, CSEC, the RCMP, CBSA, Canada Revenue Agency and the Department of Health, and the list is not exhaustive.

Section 5 of *SCISA* says that a government institution's information sharing is "subject to any provision of any other Act of Parliament, or any regulation made under such an Act, that prohibits or restricts the disclosure of information." Among the stated purposes of *SCISA* is to facilitate information sharing between government institutions to protect Canada against activities that undermine its security. <sup>10</sup> That goal is different from the purpose in the existing *Privacy Act*, but there is some overlap.

The intersection of the two Acts is most clear under the collection, use and disclosure provisions. While *SCISA* is theoretically subordinate to the *Privacy Act*,<sup>11</sup> the latter explicitly allows disclosure authorized by *any* other *Act of Parliament*,<sup>12</sup> which would permit any disclosure under *SCISA* that might otherwise be prohibited.

Since *SCISA* does not deal with collection of information by government institutions, the *Privacy Act* would presumably continue to govern, at least at first instance. It provides that

The constitutionality of sharing personal information with foreign governments has been challenged—unsuccessfully. See, *United States of America v. Lucero-Echegoyen*, 2011 BCSC 1028 and *Wakeling v. United States of America*, 2014 SCC 72.

SCISA, section 3 and ATA, 2015, section 2.

SCISA, section 5(1).

<sup>&</sup>lt;sup>12</sup> *Privacy Act*, RSC 1985, c P-21, section 8(2)(b).

personal information can be used for the reason it was collected, which must be relevant to the "operating program or activity" of the collecting institution. Information may also be used for any purpose consistent with the initial purpose. Further, information can be used pursuant to a long list of specific purposes enumerated in section 8(2). This includes any purpose authorized by another Act of Parliament or regulation, and many more.<sup>13</sup>

The *Privacy Act* does not address when information "received" or "shared" by another government institution is considered necessary, or automatically subject to the requirements that apply to information that is "collected". Accordingly, it is unclear that personal information shared under *SCISA* would continue to be covered by other protections under the *Privacy Act*.

The long list of exceptions in section 8(2) of the *Privacy Act* is made even broader by section 6 of *SCISA*, providing that once information is received under section 5, it can be used and further disclosed "to any person, for any purpose" so long as it is "in accordance with law". Information sharing is not limited to the scheduled government institutions: once information has been shared under *SCISA*, the Act would allow further sharing of information with "any person, for any purpose". This seems to allow the disclosure of information to the private sector and foreign governments, both unconstrained by the *Charter*.

#### **RECOMMENDATIONS:**

- 3. The CBA recommends clarifying the interaction of the *Privacy Act* and the proposed *SCISA*.
- 4. The CBA recommends that section 6 of *SCISA* be narrowed to not allow disclosure of information to the private sector and foreign governments.

#### H. Limited Checks and Balances

There are few effective checks and balances on information sharing in *SCISA*. The Act does not contain safeguards to ensure that shared information is reliable.

Maher Arar's experience illustrated the devastating consequences of sharing inaccurate or unreliable information. The RCMP's decision to provide raw information to US authorities about his suspected al-Qaeda affiliation was the likely cause of his transport to and torture

Section 8(2)(b); 8(2)(m)(i) and (ii) and (5).

in Syria. The Arar Commission stressed the importance of precautions to ensure that in future, information is accurate and reliable before it is shared. Omitting safeguards in *SCISA* ignores lessons learned through the Arar saga and the recommendations of the Arar Commission, and risks repeating the same mistakes. By preventing civil proceedings for disclosures made in good faith, section 9 prevents individuals who suffer damages as a result of wrongful or inaccurate disclosure from seeking redress.

Section 5(1) of *SCISA* would only authorize disclosure of information "relevant" to the recipient institution's jurisdiction or responsibilities for activities that undermine the security of Canada, "including in respect of their detection, identification, analysis, prevention, investigation or disruption." While the requirement of "relevance" appears on its face to limit the scope of information sharing, the broad definition of "activities that undermine the security of Canada" would mean almost everything is relevant. The expression "jurisdiction or responsibilities" is also so broad it could encompass almost anything.<sup>14</sup>

The other seemingly restraining feature of section 5(1) is that it is subject to any prohibitions or restrictions on disclosure in other Acts or regulations. As discussed above, we believe that restrictions on disclosure under existing laws will not effectively restrain the enhanced information sharing under *SCISA*.

While section 4(b) of SCISA states that information sharing should be guided by "respect for caveats on and originator control over shared information", these principles are unenforceable.

Finally, section 6 of *SCISA* authorizes additional disclosure "to any person, for any purpose", as long as the disclosure is "in accordance with law". This would be less problematic if it clearly applied only to sharing between Canadian agencies (which is not expressly stated).

### **RECOMMENDATION:**

5. The CBA recommends that *SCISA* include safeguards to ensure that any shared information is reliable.

<sup>14</sup> Craig Forcese and Kent Roach, *Bill C-51 Backgrounder # 3: Sharing Information and Lost Lessons from the Maher Arar Experience* at 31. Available at <a href="https://www.antiterrorlaw.ca">www.antiterrorlaw.ca</a>.

## I. SCISA Needs Effective Review and Accountability

*SCISA*'s broad intrusion on privacy lacks an oversight or review mechanism to counterbalance that intrusion. The Arar Commission recognized that the effective enforcement of legal restrictions on information sharing requires integrated and self-initiated review. Yet *SCISA* does not mention the need for an independent review body with the mandate to ensure that information sharing is reliable, relevant, and in accordance with all legal restrictions.

The Backgrounder to Bill C-51 states that *SCISA* "fulfils the Government's commitment to introduce information sharing legislation as part of the Air India Inquiry Action Plan" and that "the authority to share information proposed by this Bill is not without limit." The Backgrounder suggests that information can only be shared with designated Canadian government institutions when relevant to their national security responsibilities, and that only those officials within the institution who require the information to carry out their duties will be delegated to receive this information. It concludes by saying:

[t]he *Privacy Act*, and with it the Office of the Privacy Commissioner's authority to investigate potential violations, will continue to apply to information shared under the proposed Act. The review functions of the Office of the Privacy Commissioner and the Office of the Auditor General of Canada will help maintain an appropriate balance between protecting the privacy of citizens and ensuring national security.<sup>15</sup>

While we believe limits to the broad powers granted by Bill C-51 are critical, the limits fall far short of adequately protecting Canadians and the promises in the Backgrounder have not been verified. When Bill C-51 was released, Daniel Therrien, Privacy Commissioner of Canada, questioned the scope of the Act and its lack of oversight:

At this early stage, I can say that *I am concerned with the breadth of the new authorities* to be conferred by the proposed new *Security of Canada Information Sharing Act*. This Act would seemingly *allow departments and agencies to share the personal information of all individuals, including ordinary Canadians who may not be suspected of terrorist activities*, for the purpose of detecting and identifying new security threats. It is not clear that this would be a proportional measure that respects the privacy rights of Canadians.

...

I am also concerned that the proposed changes to information sharing authorities are not accompanied by measures to fill gaps in the national security oversight regime. Three national security agencies in Canada are subject to dedicated independent

oversight of all of their activities. However, most of the organizations that would receive and use more personal information under the legislation introduced today are not. Gaps in the oversight regime were identified long ago, notably by Justice O'Connor in the report he made at the conclusion of the Arar Inquiry [that injustice may flow from poorly controlled information sharing]. [emphasis added]

The Privacy Commissioner's jurisdiction only extends to "personal information", and may not reach all information at issue under the new sharing regime. Again, the application of the *Privacy Act* and powers of review by the Privacy Commissioner are far from clear. Even if they apply, the Commissioner himself has acknowledged the limits of the Office as an effective oversight body. <sup>16</sup> And it must be remembered that secrecy could be claimed over most national security information sharing, making oversight and review even more difficult.

#### **RECOMMENDATION:**

6. The CBA recommends that *SCISA* be amended to provide effective oversight, including regular Parliamentary review of its effects and operations.

\*\*\*

Information sharing is logical and appropriate to ensure the efficient and effective operation of government institutions as a whole. Unchecked, it is fraught with dangers for visitors to Canada and innocent Canadians, as vividly illustrated by the cases of Maher Arar and others.

*SCISA* represents a significant expansion of information sharing powers without adequate definition and clarity, and lacks basic concepts of privacy protection. Clarification of key terms and consideration of those basic concepts is urgently needed, along with sufficient information sharing controls and effective oversight. The CBA recommends that such an expansive information sharing regime be subject to Parliamentary review of its effects and operation after a certain period, commonly three to five years.

## IV. CLARIFYING RESTRICTIONS IN SECURE AIR TRAVEL ACT

Bill C-51 introduces the *Secure Air Travel Act* (*SATA*) to provide a new framework for identifying and responding to people who pose a threat to transportation security or who

www.priv.gc.ca/parl/2015/parl sub 150305 e.asp (para 3 of Oversight and Review)

may travel by air for the purpose of committing a terrorism offence. The CBA supports the government's efforts to take another look at programs designed to respond to the events of September 2001, and ensure they are securely grounded in law.

Safe air travel is vital to individual Canadians and to Canada's economy and commerce. A no fly list can contribute to public safety, and it must be workable and fair. It must be targeted to allow legitimate travellers to move freely and not unduly affect people and businesses. The criteria for inclusion in the list must be subject to direct Ministerial or Parliamentary review, and a process for removing a name from the list must be expeditious and effective, given the potential for error.

There have been problems with similar no-fly lists in the past, including the absence of information as to their effectiveness in identifying threats.

A Fact Sheet issued by the Office of the Privacy Commissioner of Canada in June 2007 states:

While we do not question the desire to make air travel more secure, it remains to be seen whether a list of this kind will in fact make air travel more secure. Transport Canada has not provided studies or evidence to show the effectiveness of no-fly lists. Despite repeated requests that such evidence be produced, the necessity and effectiveness of such a measure have yet to be demonstrated.<sup>17</sup>

The British Columbia Civil Liberties Association stated:

According to *Travelwatchlist*, in the first year of the Passenger Protect Program, Transport Canada reported approximately 100 cases of false-positive matches based on a list that is said to contain between 500 and 3,000 names. <sup>18</sup>

The US Department of Homeland Security recognized the potential for errors in their system, by analysing false positives (where an innocent person is identified as being on the list), and false negatives (where a real threat to security is not included).<sup>19</sup> They

www.priv.gc.ca/resource/fs-fi/fs 20070627 e.asp

http://bccla.org/privacy-handbook/main-menu/privacy7contents/privacy7-1-4/

In the *Annual Report* to Parliament 2007-2008, the Privacy Commissioner noted that in the US, children and public figures were on the list and subsequently encountered questioning or were denied boarding (eg. US Senator Edward Kennedy).

determined that a system sensitive to false negatives will necessarily produce a large number of false positives.<sup>20</sup>

Jennifer Grover, Acting Director, Homeland Security and Justice in the US Government Accountability Office, told the House of Representatives:

However, we found that Secure Flight does not have measures to assess the extent of system matching errors—for example, the extent to which Secure Flight is missing passengers who are actual matches to these lists...We also found in September 2014 that TSA lacks timely and reliable information on all known cases of Secure Flight system matching errors.<sup>21</sup>

Canada has had a Passenger Protect Program (more often called a no fly list) since 2007, to deny air travel to those deemed to be an immediate threat to aviation security. Bill C-51 would clarify and expand the basis for denying air transportation to people perceived as threats, adding certainty as to when air travel can be denied. While added certainty is beneficial, the proposals may unduly interfere with the legitimate personal and business travel of Canadians. Under Bill C-51, a person may be denied travel based on a mere possibility of risk, determined by an unknown person and using unknown and untested criteria.

- The proposed system is likely to produce false positive matches, as only basic information about individuals will be on the no-fly list. Section 8(1) only requires the given name, surname, known alias, date of birth and gender of the person.
- The criteria for placing a person on the no-fly list are unclear. While the criteria used to establish a no-fly list or place a person on it should not be disclosed to prevent any attempts to circumvent them, what it takes to be put on the list must be objectively discernible. Information relied on must be tested by responsible authorities and be reliable. The criteria used in domestic policing may not be wholly applicable to intelligence gathering, but both spheres need to determine the reliability of information and whether it can be acted on.
- *SATA* could interfere with other civil liberties as well. Sections 28 and 30 would introduce powers to search computers and mobile devices without warrant, and without

<sup>20</sup> Report on Effects on Privacy and Civil Liberties, Department of Homeland Security, April 27, 2006.

<sup>&</sup>lt;sup>21</sup> See, GAO - 14 - 796T, at 6.

oversight.<sup>22</sup> A personal computer, or mobile device, contains a significant amount of personal information, for example, personal health information or photographs that should not be accessed without judicial supervision in the form of a warrant, or, at a minimum, oversight of the process. Computers or mobile devices of lawyers are likely to contain privileged client information.<sup>23</sup> The US Department of Homeland Security developed a policy in 2009 to address this important problem.<sup>24</sup> More, section 30 seems to allow warrantless searches against any person who happens to be present in an airport or other aviation facility. These powers are potentially overreaching and unconstitutional in allowing access to personal or privileged information without lawful authority.

- There is a *lack of safeguards for those wrongly placed on the list*. Section 8(2) provides that the Minister review the list every 90 days to decide if a person should remain on it. Yet, no objectively discernible basis for removing a name is provided.<sup>25</sup> There is no process for expeditious determination by the Minister (or for appeal) because of urgent or exigent circumstances for a person denied flight, such as medical or compassionate grounds, going abroad for employment purposes or to visit a dying relative.
- Section 15 requires the Minister to give a person denied travel the opportunity to make submissions, but *individual applicants are not entitled to any information as to why they were put on the list*. Without a requirement to provide meaningful information, the administrative recourse in Bill C-51 is illusory.
- Similarly, the *appeal process may be less than ineffective*. Any appeal to the Federal Court can occur only after all administrative remedies have been exhausted, meaning significant delay and expense. The reviewing judge will determine if the decision of the Minister or delegate is reasonable, but the government may insist that an applicant be excluded from that hearing. The judge may decide a case based on undisclosed

<sup>&</sup>lt;sup>22</sup> See, *R. v. Fearon* 2014 SCC 77 at para 51.

The search of cell phones, like the search of computers, implicates important privacy interests that are different in nature and extent from other searches: see, *R. v. Vu*, 2013 SCC 60 (CanLII), [2013] 3 SCR 657, at paras. 38 and 40-45. In a letter to the Ministers of Justice and Public Safety, dated June 19 2014, the CBA expressed its concerns on this topic, and offered our assistance in developing a Canadian policy.

www.dhs.gov/xlibrary/assets/privacy/privacy pia cbp laptop.pdf

In *Ibrahim v. Department of Homeland Security*, Case No. C06-00545, United States District Court, for the Northern District of California, a scholar had been placed on the no-fly list because an FBI agent filled out a form incorrectly. It took years of litigation to remove her name.

evidence, and not even a summary must be disclosed to the affected party. There is no provision for a special advocate to act on behalf of the applicant, as in security matters.

#### **RECOMMENDATIONS:**

#### 7. The CBA recommends:

- providing an objectively discernible basis for additions to and removals from the no-fly list,
- curtailing warrantless search powers, and
- adding effective safeguards for those wrongly placed on the list, including a process for expeditious removal.

## V. MAKING BETTER USE OF THE CRIMINAL CODE

## A. What it means to "Advocate or Promote" Terrorism

Bill C-51 proposes a new offence of advocating or promoting terrorism:<sup>26</sup>

83.221. Every person who, by communicating statements, knowingly advocates or promotes the commission of terrorism offences in general – other than an offence under this section – while knowing that any of those offences will be committed or being reckless as to whether any of those offences may be committed, is guilty of an indictable offence and is liable to imprisonment for a term of not more than five years.

The CBA supports legislative changes to make Canadians safer and that are consistent with Canada's legal traditions and constitutional principles. We believe that the proposed new offence fails to meet these tests.

Terrorism offences are crimes against the population and those who commit them must be treated as criminals. Before 2001, Canada experienced occasional acts that we would today

Under international law, *Bosnia and Herzegovina v Serbia and Montenegro* [2007] ICJ 2, deals with "incitement" to genocide, rather than 'advocating' and 'promoting' genocide.

The Council of Europe Convention on the Prevention of Terrorism (2005), Council of Europe Treaty Series No. 196 [European Convention], the most comprehensive regional convention to date, addresses public provocation to commit a terrorist offence (Article 5), recruitment for terrorism (Article 6), and training for terrorism (Article 7). A fourth provision on accessory (ancillary) offences (Article 9) was added with the stipulation that certain acts (defined as crimes in one of the counter-terrorism treaties listed in the Convention's appendix) must not be actually committed to constitute a crime.

call "terrorist acts" and effectively dealt with them as crimes.<sup>27</sup> Those who engage in terrorist crimes have always been subject to heavy penalties, with an emphasis on denunciation and deterrence, but within the scope of the criminal justice system. There is no separate sentencing regime for these acts.<sup>28</sup> The CBA sees no evidence of a lack of sentencing tools in the *Criminal Code* calling for a departure from established principles or practices of the criminal justice system in prosecuting these offences.

A primary principle of criminal law is that people must know in advance what conduct is prohibited and what permitted. As stated by the Supreme Court of Canada in *R. v. Kelly*:

It is a fundamental proposition of the criminal law that the law be certain and definitive. This is essential, given the fact that what is at stake is the potential deprivation of a person of his or her liberty...there must be no crime or punishment except in accordance with law which is fixed and certain.<sup>29</sup>

In contrast to this required certainty, section 83.221 appears to apply to all "statements", which could include private statements, emails and text messages. Unlike the similarly structured child pornography and hate propaganda offences, there is no exemption for private conversations.

Further, the proposed offence refers to "terrorism offences *in general*" (emphasis added), rather than simply "terrorist activity". This signals a deliberate intent to cast the net both broadly and vaguely. It would include existing terrorism offences, as well as any other indictable offence committed for the benefit of, at the direction of, or in association with a terrorist group. It is impossible to know in advance the scope of prohibited conduct.

If not intended to significantly expand the scope of the criminal law, there is no need for a new section that duplicates section 22 of the *Criminal Code*, which prohibits counselling an offence. "Advocates" and "promotes" are also undefined, though there is some judicial authority defining these words. We do not know how broadly these provisions will be interpreted, but again, certainty is essential in criminal law.

The gap this new offence is intended to fill is unclear, given that direct incitement of terrorist acts (as opposed to "terrorism offences in general") is already a crime. Speech that

For example, those responsible for bombing the Litton plant in Mississauga, Ontario in 1982 were sentenced to long terms of imprisonment for that and other criminal activity.

<sup>&</sup>lt;sup>28</sup> R. v. Khawaja, [2012] 3 SCR 555, 2012 SCC 69 (CanLII), at para. 130.

<sup>&</sup>lt;sup>29</sup> [1992] 2 S.C.R. 170, per McLachlin, J., concurring.

incites crime is not constitutionally protected, but the breadth of this proposal suggests that it could infringe on *Charter* protections of free speech.

For example, if apartheid still existed in South Africa, and Nelson Mandela was still a prisoner, a person at a rally in Toronto may call for dismantling that regime and urge support for the African National Congress (ANC). If, after addressing the crowd, some attendees decided to send money to the ANC, the speaker could be guilty of "advocating terrorism in general" under Bill C-51. While the ANC was a political movement, it also had a military wing that carried out attacks on South African military and police targets. The speaker may have called for actions against an apartheid state, but knowing of the ANC's military capacity and still advocating support for the organization could run afoul of the new offence in Bill C-51, as a terrorism offence "in general".

This could apply to other situations where one country occupies another. Support for Israeli fighters who wanted to overthrow the British mandate in Palestine could be caught, as could those opposed to the Soviet occupation of Afghanistan. Changing political situations around the world should not dictate what will be considered terrorism under Canadian law, or what "terrorist offences in general" are. Greater certainty is needed than the proposals in Bill C-51.

There are no public interest or education defences, as there are for promotion of hate or child pornography offences, models for the proposed offence. We question whether journalists or academics could be subject to prosecution under the new offence.

Even a private academic conversation where a person voices support for an insurgent group could be caught. Such a broad limitation on free speech could be found unconstitutional. Even if charges are never brought in inappropriate situations, the result could be a significant chill on free speech, undermining our democratic order.

The standard for prosecution for the proposed offence is very low. A person need not intend that any specific offence be committed, nor any person or place be endangered. They need only know or be reckless as to whether an offence *may* be committed. In other words, the person must simply be aware that someone hearing or reading a statement *may* commit a terrorism offence as a result of that communication – the person need not "will" or "intend" that outcome.

This is a departure from similar offences in the *Criminal Code*, such as *wilfully* promoting hatred. The use of the word "may" could capture situations where there is only a *mere possibility* that a terrorism offence will be committed. Further, Bill C-51 would not require a direct or substantial connection between the person making a statement and the person who carries out an offence. The CBA believes this is too low a standard for criminal culpability, particularly when combined with the vagueness of the "in general" provision.

The "recklessness" standard in the proposed offence may violate section 7 of the *Charter*. Given the stigma associated with terrorism offences, actual knowledge or wilful blindness should be required. This is bolstered by the fact that the offence only requires the accused to be reckless to the possibility that a terrorism offence *may* be committed. The combination of the recklessness standard and the word "may" in section 83.221 sets the *mens rea* requirement too low.

Finally, there must be a clear answer as to what the proposed offence would actually contribute to public safety. There is little evidence that prohibiting extreme speech will prevent terrorist activity. The chill on free speech may drive extremist communications underground, where it is more difficult to monitor or detect. Further, anti-radicalization often depends on frank engagement between authorities, communities and parents. Outreach may require the type of "extreme dialogue" targeted by the Bill to address beliefs and emotions that lead to radicalization.

Criminal acts can only be detected and prevented by allocating sufficient resources to law enforcement. Police work, intelligence gathering and sharing information with allied states and agencies, all subject to coherent review mechanisms, are better ways to combat those who would commit terrorist crimes than introducing an offence that is too vague and unlikely to withstand constitutional challenge.

If narrowly construed by the courts, the proposed section will add nothing to existing offences such as counselling the commission of an offence, advocating genocide, or contributing to a terrorist organization. If widely construed, it will be subject to challenges, at cost to taxpayers, and may include activity more political in nature than dangerous.

#### **RECOMMENDATION:**

8. The CBA recommends that the proposed section 83.221 be deleted from Bill C-51.

## **B. Properly Targeting Terrorist Propaganda**

Bill C-51's proposed section 83.222 of the *Criminal Code* would introduce the concept of "terrorist propaganda", and proposed section 83.223(5) would authorize a judge to order the deletion of "terrorist propaganda" from the internet if it is "available to the public". Terrorist propaganda is defined as "any writing, sign, visible representation or audio recording that advocates or promotes the commission of terrorism offences in general ... or counsels the commission of a terrorism offence". In this way, the proposed deletion orders are linked to the proposed new offence of advocating or promoting terrorism. The CBA supports the concept of deletion orders for terrorist propaganda in principle. However, we share concerns expressed by Professors Roach and Forcese about the formulation in Bill C-51:

- The definition is overly broad, using much of the same language as the new advocating terrorism offence.
- There is no mental fault requirement: a deletion order may be made even if the author had no intent or awareness that the material was "terrorist propaganda".
- Like the offence of advocating or promoting terrorism, the definition of terrorist propaganda does not include public interest, education or religious discussion defences. Academic or political commentary only indirectly connected with anything that could be called violent may be considered "terrorist propaganda" and subject to a deletion order. Censorship to this degree is harmful to Canada's democracy and likely to elicit constitutional scrutiny.
- The deletion order scheme presents practical difficulties. Section 83.223(2) creates an adversarial process by requiring the judge to give notice of an application for a deletion order to the publisher or author. That person must have the opportunity to show cause why the material should not be deleted. In practice, the person who created or posted the material may be afraid to challenge the application, for fear of being arrested for the offence of knowingly promoting or advocating terrorism offences. As a result, many hearings would be one-sided. Also, there is no appeal from deletion orders made in one-sided hearings where the individual is not present.<sup>30</sup>

The CBA recommends some amendments to correct these issues.

Craig Forcese and Kent Roach, *Bill C-51 Backgrounder #4: The Terrorism Propaganda Provisions* (Feb. 23, 2015). Available at: <a href="https://www.antiterrorlaw.ca">www.antiterrorlaw.ca</a>.

#### RECOMMENDATIONS:

- 9. The CBA recommends that the definition of "terrorist propaganda" be limited to material that counsels the commission of a terrorist offence or that instructs the commission of a terrorist offence.
- 10. The CBA recommends the proposed deletion orders for "terrorist propaganda" include a mental fault requirement, and defences to exclude legitimate public interest, education or religious discussion activities.
- 11. The CBA recommends allowing judges to appoint *amicus curiae* to address appeals of the proposed deletion orders.

In practice, the new deletion orders are unlikely to be used frequently, and security officials are more likely to ask internet service providers to voluntarily delete controversial material. These informal approaches would not be subject to judicial supervision but risk undermining freedom of expression.

A consequential amendment would add "terrorist propaganda" to a customs tariff that allows warrantless seizure and detention of obscenity and hate propaganda at the border. Given the uncertainty around and broad scope of what will be considered "terrorist propaganda", this new power could be misunderstood or misused by the Canadian Border Service Agency (CBSA). This problem is compounded because the CBSA is not subject to any independent review body. The CBA has recently called on the federal government to implement an independent and effective complaints and monitoring mechanism for the CBSA.<sup>31</sup>

#### **RECOMMENDATION:**

12. The CBA recommends that the consequential amendment to the customs tariff be deleted.

## C. Preventive Detention is an Extraordinary Measure

With the introduction of Canada's first anti-terrorism laws came extraordinary powers of preventive detentions and investigative hearings. Operating from 2001 to 2007 (the five year sunset clause expired in 2007) and then again after 2012, the preventive arrest provision allows police to arrest someone they suspect will commit a "terrorism" offence

when they lack evidence to charge the person with any offence. The rationale is to disrupt and prevent terrorist offences by short-term detention if certain requirements are met. It is premised on averting an imminent and serious terrorist threat where evidence is lacking for reasonable and probable cause for arrest and charge for a criminal offence. The CBA supports these reasonable and grounded objectives, subject to proper limitations and oversight.

Under existing law, a peace officer may arrest and detain a person if there are reasonable grounds to believe that a terrorist activity will be carried out and reasonable grounds to suspect that imposing a peace bond is necessary to prevent the terrorist activity. The provision currently allows for 72 hours of detention before a judge considers imposing a peace bond on the person. The person cannot be held longer unless they refuse to agree to the conditions of the recognizance. If so, they may be committed to prison for up to 12 months.

Canadian experience as to whether the preventive detention provision in section 83.3 is necessary or effective is lacking. Previous Parliaments have recognized its extraordinary nature by attaching sunset clauses.

Bill C-51 would reduce the legal thresholds in its potential application, extend the permissible period of preventive detention, and omit a sunset clause. It would make permanent what was once justified as a temporary and exceptional legal measure, and make this extraordinary legal measure more robust. This is all without evidence to show that changes are warranted.

Section 17 replaces the current requirement of a reasonable belief that "terrorist activity will be carried out" with a reasonable belief that terrorist activity "may be carried out". It also replaces the requirement that a recognizance or arrest of a person "is necessary to prevent the carrying out of the terrorist activity" with "is likely to prevent the carrying out of the terrorist activity." The previous wording "will" and "necessary" combined with the requirement of "reasonable grounds to believe" and "proof on balance of probabilities" is an adequate basis for judges to balance societal protection with individual liberty. The lower standard proposed in the Bill could upset this balance.

The Bill would extend the maximum period of preventive detention from three to seven days. We see no need for this. Finally, section 83.3(12) may be problematic given its overly broad and vague definition of "terrorism" or "terrorist activity".

#### **RECOMMENDATION:**

13. The CBA recommends that Bill C-51 retain existing legal thresholds for preventive detention and permissible periods for detention, and include a sunset clause.

## D. Use Peace Bonds Instead of Control Orders

Section 24 of Bill C-51 proposes removing the words "or a terrorism offence" from section 810.01(1). Currently, this provision adapts the peace bond scheme in section 810 of the *Criminal Code* to offences of intimidation, criminal organization, and terrorism.

The Bill proposes a new section 810.011 for peace bonds in the context of a terrorism offence, with a significantly lower standard. Section 810.01(1) currently provides for a peace bond where a person fears, on reasonable grounds, that another person "will" commit a terrorism offence. Proposed section 810.011(1) uses "may" commit a terrorism offence. The CBA supports this reduced standard as an effective way to ensure the timely disruption of possible terrorist threats.

The proposed section 810.011(1) would also increase the maximum duration of a peace bond from two years to five years if the judge is satisfied that the person was previously convicted of a terrorism offence. Finally, it would require the judge to consider several broader conditions, including that the individual give up any passport and remain in a specified geographic area.

This proposed section is redundant and unnecessary. Section 810.01(1) already addresses terrorism offences. Amendments that seek a recognizance for a period of up to five years if a person has been convicted previously of a terrorism offence, and the addition of broader conditions, could all be incorporated by amendment in the existing sections or framework.

The increase of up to five years for a recognizance on a person previously convicted of a terrorism offence may be susceptible to constitutional challenge. It would prolong and complicate proceedings as courts determine whether a previous conviction was for a "terrorism offence", given uncertainty and vagueness around the legal of definition "terrorism".

#### **RECOMMENDATION:**

14. The CBA recommends that, instead of introducing a new regime for control orders, the current section 810.01(1) be retained, and amended if required to better address terrorism offences.

# VI. MONITORING NATIONAL SECURITY, INCLUDING CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS)

## A. Kinetic powers require oversight

One of the most concerning changes in Bill C-51 is the proposed transformation of CSIS from an intelligence-gathering agency to one actively engaged in countering national security threats. The addition of kinetic intervention to the CSIS mandate would fundamentally transform the agency. The CBA is concerned about the scope of the additional mandate and the lack of accountability and oversight commensurate with the agency's new role.

CSIS could employ undefined "measures" "within or outside of Canada" to "reduce" a "threat to the security of Canada". The threshold for using those measures would be "reasonable grounds to believe a particular activity constitutes a threat to the security of Canada".

CSIS received an expansive mandate in its founding statute, a concern that was raised at the time of its creation.<sup>32</sup> CSIS powers have always depended on how a "threat to the security of Canada" is defined, and an extremely broad definition is included in section 2 of the *CSIS Act.* Based on reports of CSIS surveillance activities in past years, the expansive definition of "threats to the security of Canada" appears to have been interpreted to include environmental activists, indigenous groups and other social or political activists.<sup>33</sup> While this is troubling for an intelligence agency, our concerns are significantly heightened with the proposal to grant CSIS a "disruptive" kinetic role.

Limits on CSIS's new kinetic powers proposed in Bill C-51 include sections:

<sup>32</sup> www.parl.gc.ca/Content/LOP/researchpublications/8427-e.htm#E.%20The%20Controversial

 $<sup>\</sup>frac{www.theglobeandmail.com/news/politics/anti-petroleum-movement-a-growing-security-threat-to-canada-rcmp-say/article 23019252/$ 

www.theguardian.com/environment/2013/feb/14/canada-environmental-activism-threat

- 12.1(2) "measures" are to be "reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat";
- 12.1(3) CSIS must not take any measures that will violate the *Charter* or any other Canadian law unless a warrant is issued under the proposed section 21.1; and
- 12.2 CSIS is prohibited from causing death or bodily harm to an individual, wilfully attempting to obstruct, pervert or defeat the course of justice, or violating the sexual integrity of an individual.

The CBA believes that these restrictions are not enough. Practically speaking, whether the measures are "reasonable and proportional" will be decided unilaterally within government and CSIS. CSIS only needs a warrant under section 21.1 if it has "reasonable grounds" to believe that it is required, and a warrant is only required where the measures "will" (not "may") contravene a *Charter* right or a Canadian law. Measures that do not meet this threshold require no judicial warrant and the applicable oversight would be only internal or executive branch controls.<sup>34</sup> As one example, the proposed amendments would allow CSIS to provide misinformation to foreign environmental funders to deter them from funding Canadian environmental groups opposed to pipeline projects.

Enhanced CSIS powers may also present operational problems. For example, it is unclear how CSIS's new kinetic powers would affect a subsequent criminal trial. CSIS operations that occur prior to a criminal investigation may overlap, affect and taint a subsequent RCMP investigation and evidentiary record. Further, the criminal trial may be delayed by questions and applications arising from Federal Court warrants and *Charter* violations. CSIS kinetic operations may actually make prosecutions more difficult.

The proposed expanded CSIS powers will further overlap with RCMP powers. The Air India Commission recognized the importance of cooperation and information sharing between CSIS and the RCMP to effectively address terrorist threats, and recommended a national security advisor to settle disputes and ensure that intelligence is shared between CSIS and other security agencies and departments. This recommendation has not been implemented, and without a body overseeing all national security operations, the overlap between the

Craig Forcese and Kent Roach, *Bill C-51 Backgrounder #2: The Canadian Security Intelligence Service's Proposed Power to "Reduce" Security Threats through Conduct that May Violate the Law and the Charter* (February 12, 2015). Available at <a href="www.antiterrorlaw.ca">www.antiterrorlaw.ca</a>.

proposed CSIS powers and the RCMP mandate could lead to confusion and inefficiency.

Justice Major, who headed the Air India Commission, has recently pointed to this problem:

They may be entitled to do more than simple intelligence gathering," he said of CSIS under the proposed new law. "If that's the case, it can lead to other problems of overlap. The RCMP get a little annoyed and think, 'Well, let CSIS do it.' And CSIS doesn't do it. When you have that many agencies involved, it's a recipe for confusion unless there's somebody steering the ship.<sup>35</sup>

Proposed section 12.1(3) combined with the warrant provisions in section 21.1 is also of concern to the CBA, as it is unclear to what extent it would direct judges to authorize contraventions of Canadians' constitutional rights under the *Charter*. It appears that the sections would empower the Federal Court to authorize "measures" such as:

- working with Foreign Affairs and CBSA to prevent the return of a citizen feared to pose a potential future risk of political violence (contrary to section 6 of the *Charter*),
- seizing or deleting a website which CSIS believes may encourage support for a foreign insurgency (contrary to section 2(b) of the *Charter*), and
- possibly even detaining individuals believed to be a "threat to the security of Canada" (despite sections 9, 7, 10, and 12 of the *Charter*).

While the government has repeatedly indicated that the new CSIS powers would not extend to arbitrary detention, there are no express limits excluding detention. Detention would not come within the restrictions of obstructing justice or violating sexual integrity, nor does it constitute bodily harm. Further, it is unclear whether "bodily harm" includes psychological harm in the proposed section 12.3, and if it does not, CSIS may be empowered to seek authorization to conduct psychological torture (contrary to section 12 of the *Charter*).<sup>36</sup>

#### **RECOMMENDATION:**

15. The CBA recommends the creation of an Office of the National Security Advisor, to act as an expert review body with resources and a mandate to review *all* national security activity, and to ensure effective information

www.theglobeandmail.com/news/politics/ottawa-didnt-learn-air-india-lesson-says-exjudge/article23240705/

<sup>&</sup>lt;sup>36</sup> R. v. McGraw [1991] 3 S.C.R. 72.

sharing and cooperation between CSIS and other security agencies, including the RCMP.

16. The CBA recommends amending section 12.2 to prohibit CSIS from arbitrarily detaining an individual and to clarify that "bodily harm" includes psychological harm.

## B. Judges should not authorize Charter Violations

Proposed sections 12.1(3) and 21.1 appear to provide for judicial warrants to authorize the violation of *any Charter* rights. This brings the entire *Charter* into risk, and is unprecedented.

Judicial warrants for search and seizure are intended to *prevent*, not *authorize*, *Charter* violations. This is because the *Charter* protection against search and seizure is qualified: it only protects against "unreasonable" search and seizures. A judge authorizing a search does not authorize a breach of the *Charter*, but authorizes the search to prevent what would otherwise be a breach of the section 8 protection from unreasonable search and seizure.

Other *Charter* rights, such as the right against cruel and unusual punishment or mobility rights, are absolute, and their violation can never be "reasonable". While all *Charter* rights are subject to reasonable limits under section 1 of the *Charter*, any restraint on the right is usually clearly set out in advance in legislation. Even section 25.1 of the *Criminal Code*, allowing the police to break laws of Parliament in certain circumstances, does not purport to authorize breaches of the *Charter*:

To imagine that a court can pre-authorize a violation of a right in response to an open-textured invitation to do so is to misunderstand entirely the way our constitution works, on a fundamental level. ... This is an astonishing rupture with foundational expectations about both the rule of law and the role of the judiciary.<sup>37</sup>

This aspect of the proposed Bill is at odds with the role of the courts and the judiciary. Canada's judges are charged with upholding the Rule of Law and Canada's *Constitution* against unlawful state action. They should not be conscripted by the state to limit *Charter* rights, when their fundamental role is to ensure that all legislation is in accordance with the *Constitution* and prevent unjustified *Charter* violations.

<sup>37</sup> 

The proposed sections 12.3 and 21.1 could authorize any conduct that violates the *Charter* in the name of reducing a threat to the security of Canada, as long as it does not obstruct justice, cause bodily harm, or violate sexual integrity. This invitation to *Charter* violations is unlikely to be justified under section 1 or to be interpreted as being "prescribed by law".

There are also procedural concerns with this proposal. Any deliberation on the fundamental question of when and how CSIS can be authorized to violate *Charter* rights will be conducted in an *ex parte* and *in camera* warrant proceeding. The hearing will be conducted in secret, and only the government's views will be represented. No third parties will be able to make submissions. Further, the ultimate court decision will likely be unavailable to the public, due to confidential security information. No party will be able to appeal the decision.

It is untenable that the infringement of *Charter* rights is open to debate, in secret proceedings where only the government is represented.

Without a clear articulation of Parliamentary intent in considering this remarkable step, the CBA is unable to provide more meaningful commentary on the scope of the proposed warrants. However, we do not support the proposition that Parliament could empower CSIS or judges to disregard the constitutional foundations of our legal system.

#### **RECOMMENDATION:**

17. The CBA recommends that the judicial warrant provisions in sections 12.1(3) and 21.1 of Bill C-51 be amended to ensure that they align with the fundamental role of Canada's judiciary in upholding the Rule of Law and Canada's constitutional guarantees.

# C. CSIS should be bound by the Charter

Section 12.1(3) only requires CSIS to request a warrant for measures that *will* contravene a *Charter* right. In the context of criminal investigations, there is an impetus under current law for police to be cautious in any activities that *may* infringe *Charter* rights, given the impact of a breach on any potential prosecution. In the context of intelligence gathering and "disruption" of national security threats, the institutional impetus for caution may not be the same, even though officers act with the best intentions. CSIS has been the subject of

several recent reports, as well as decisions from the Federal Court, indicating the perception of a lack of candour on the part of the Service behind closed doors.<sup>38</sup>

## D. Need for Oversight and Review

We underscore the distinction between "oversight" and "review": oversight is command and control over operations (in other words, real time governance), while review is retrospective auditing of operations, measured against a set of criteria. In relation to CSIS, the Security Intelligence Review Committee (SIRC) performs review, while the executive branch of government and the judiciary perform oversight.

We have significant concerns around the oversight and review of kinetic operations by CSIS. The *Arar* Commission and others have made clear recommendations about shortcomings of the current oversight and review regime of the national security apparatus.<sup>39</sup> As many of those recommendations have yet to be implemented, expanding national security powers without a corresponding reinforcement and expansion of an insufficient oversight and review regime is a serious problem.

First, there is already a lack of effective executive oversight over CSIS operations. There is evidence that CSIS does not keep the Minister of Public Safety properly informed of its activities. The Air India Commission<sup>40</sup> was concerned with the efficacy of executive oversight of CSIS, and recommended that CSIS not have unreviewable discretion to withhold relevant intelligence from others in government. This recommendation has not been implemented.

Second, judicial oversight is limited. Judicial warrants are only required for some proposed CSIS powers. Bill C-51 specifies that CSIS need only seek a warrant where it has "reasonable grounds" to believe that it is required. And a warrant is only required if measures "will" – not "may" – contravene the *Charter* or another Canadian law. Measures that fall short of violating the *Charter* or another law do not require a warrant, so there is no judicial oversight. This suggests that there will be little or no judicial oversight of CSIS activities abroad, where the application of Canadian law and the *Charter* are less than clear.

www.sirc-csars.gc.ca/pdfs/cm\_arar\_bgv1-eng.pdf

Arar Commission, Volume 1: section 3.1.1.6 Sharing Information with Foreign Agencies (link to volume 1: www.sirc-csars.gc.ca/pdfs/cm arar bgv1-eng.pdf

http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/air /2010-07-23/www.majorcomm.ca/en/reports/finalreport/default.htm

Even where CSIS seeks a warrant, the new warrants may authorize unprecedented CSIS powers, again, including *Charter* breaches. In these circumstances, it is troubling that the judge is likely to not have all relevant information and constitutional arguments in making a decision. Also unlike other types of warrants, there would be no review of the warrant in open court after it is issued and executed. It is likely instead that the CSIS powers will be exercised in secret, and any information relating to the warrant will be kept confidential for national security reasons.

Third, SIRC review is limited. It does not have the resources or capabilities to effectively review CSIS action, and this problem will be compounded if CSIS is given the proposed kinetic powers. SIRC's review of CSIS activities has always been partial – it does not and cannot review every activity but rather a sampling of such activities. If the Bill is passed,

[t]he modest number of reviews SIRC can currently conduct will be spread over a greater range of activities. SIRC, under resourced at present, will be spread even thinner, meaning that it may be hard pressed to maintain its current level of scrutiny of intelligence operations while at the same time hard pressed to truly review CSIS's kinetic conduct.<sup>41</sup>

This problem will be exacerbated because the Bill would grant CSIS kinetic powers overseas: "The prospect of a resource strained, understaffed review body now being obliged to extend its reach into (expensive) extraterritorial reviews that now involve not just intelligence gathering but kinetic activities is daunting and gravely concerning." 42

Finally, SIRC's review functions are confined to CSIS action. In its 2012-2013 *Annual Report*, SIRC noted data sharing has become routine as technological barriers between information systems and databases have fallen. This technological interconnectivity requires legislative tools to allow SIRC to review CSIS activities that cross over with other agencies and departments, which Parliament has not enacted. And the problem could be worsened under Bill C-51.

Proposed section 22.3 allows other persons to assist CSIS-authorized operations. A judge may order that the assistance is confidential under the proposed section 22.3(2). It is unclear whether SIRC will be able to examine and review the actions of persons or institutions that assist CSIS. If SIRC review is confined to CSIS itself, some state conduct

Supra, note 34 at 33.

<sup>42</sup> Ibid.

authorized under the new assistance orders will be effectively unreviewable. Like the Arar Commission and others, the CBA agrees that an expert review body must be created with resources and a mandate to review *all* national security activity. The CBA also recommends the creation of a Parliamentary review committee with access to secret information. The CBA made this call, unfortunately to no avail, when the *Anti-terrorism Act* was first introduced in 2001.<sup>43</sup>

#### RECOMMENDATION:

18. In addition to the creation of an Office of the National Security Advisor, above, the CBA also recommends the creation of a Parliamentary review committee with access to secret information.

## E. Robust Reporting means Better Protection

Bill C-51 proposes adding section 6(5) to the *CSIS Act*, which would require that reports on kinetic operations and the nature of the operations be made only to the Minister and SIRC. Confidence in our intelligence services and to a robust democracy requires informed public debate on the nature and scope of kinetic operations by Canada's security services. This is particularly true if courts are asked to authorize *Charter* violations under section 21.1. Although the Bill proposes an annual SIRC report on the number of warrants issued and denied under section 21.1, the reports would not require any information about the nature of the activities authorized. More disturbingly, the Bill does not require reporting of CSIS activities under section 12.1, if they do not breach *Charter* rights or otherwise require a warrant.

#### RECOMMENDATION:

19. The CBA recommends that if CSIS mandate is expanded to engage in kinetic operations, the agency be subject to regular reporting requirements as to the nature and number of those operations, perhaps to the expert review body recommended above, whether pursuant to section 12.1 or to warrants under section 21.1.

<sup>43</sup> 

## F. Parliamentary Review of Law

Given the significance of the changes proposed in this Bill, the CBA recommends that it be brought back to Parliament for review after three or five years. Similar provisions were included in the original *CSIS Act* and in the 2001 *Antiterrorism Act*.

#### **RECOMMENDATION:**

20. The CBA recommends that Bill C-51 be brought back to Parliament for rigorous review after three or five years.

# VII. MAKING BETTER USE OF THE IMMIGRATION AND REFUGEE PROTECTION ACT

# A. Ensuring Effectiveness of Special Advocates

The special advocate regime was created to address the challenge of balancing constitutional rights of persons subject to security certificates with the public interest in national security and the secrecy often required for work in that area. Special advocates are security-cleared lawyers who may initially communicate freely with the person concerned, but not after having access to secret information and evidence, except by special order of the Court. They are prohibited from disclosing any of the secret evidence.

There are two aspects to the role of the Special Advocate. They help ensure a person concerned knows the case against them, by arguing in favour of further disclosure (whether by release of actual information in its original form or by working with Minister's counsel and the Court to summarize that information). This disclosure, including exculpatory information and items raising questions about the credibility or reliability of the Minister's information, allows the person concerned to challenge the allegations in a process that is closer to the full fairness provided by total disclosure. The Special Advocate can also make legal and factual arguments on behalf of the individual, referencing the secret material, in closed proceedings.

The Supreme Court upheld the special advocate regime in *Harkat*, <sup>44</sup> but it remains a delicate balance of interests. The Court was clear that there are limits as to how far secrecy can be pushed when an individual's *Charter* rights are at stake.

<sup>44</sup> Canada (Citizenship and Immigration) v. Harkat, 2014 SCC 37.

The use of secret evidence and Special Advocates is a substantial departure from fundamental principles of Canada's judicial system, including the principle that courts operate openly and publicly. In the 2007 decision in *Charkaoui*, 45 the Supreme Court accepted that national security concerns could require procedural modifications including limits on the open court principle. However, those modifications "cannot be permitted to erode the essence of section 7" and that "meaningful and substantial protection" was required to satisfy the section. 46

The *Immigration and Refugee Protection Act (IRPA)* requires a judge to prevent disclosure of any information if "its disclosure would be injurious to national security or endanger the safety of any person".<sup>47</sup> The Minister is required to give "all information and other evidence that is provided to the judge" to the Special Advocate.<sup>48</sup> In the security certificate context, that includes "the information and other evidence on which the certificate is based".<sup>49</sup> If the Minister applies for non-disclosure in a proceeding before the Immigration Division or Immigration Appeal Division,<sup>50</sup> or during a judicial review,<sup>51</sup> the decision-maker may appoint a Special Advocate on similar terms.

In addition to the information the Minister has relied upon, the Supreme Court's 2008 *Charkaoui* decision<sup>52</sup> expanded the scope of information for the judge to assess. *Charkaoui II* disclosure was defined in a 2009 decision by Justice Dawson as follows:

Such disclosure, it is to be remembered, consists of disclosure to the designated judge and the special advocate of *all of the information in the possession of the Service concerning the named person.*<sup>53</sup>

<sup>45</sup> Charkaoui v. Canada (Citizenship and Immigration), 2007 SCC 9, [2007] 1 S.C.R. 350. (Charkaoui I).

<sup>46</sup> *Ibid*, para. 27.

See various paragraphs of *IRPA*, section 83(1). On at least two occasions, a judge has interpreted this as *possibly* requiring the exclusion of even the Special Advocates from proceedings. In *Almrei (Re)*, 2009 FC 314, Justice Mosley acknowledged that there may be specific, narrow circumstances in which the judge would have to hear evidence in the absence of Special Advocates, but that even in such instances, "the Court must find the means to ensure meaningful participation by the special advocates" (para. 33).

<sup>48</sup> *IRPA*, section 85.4(1).

<sup>49</sup> *IRPA*, section 77(2).

<sup>50</sup> IRPA, section 86.

<sup>51</sup> *IRPA*, section 87.1.

<sup>52</sup> Charkaoui v. Canada (Citizenship and Immigration), [2008] 2 SCR 326, 2008 SCC 38.

<sup>&</sup>lt;sup>53</sup> Almrei (Re), [2010] 2 FCR 165, 2009 FC 240, at para. 43 [emphasis added].

The Special Advocate regime and *Charkaoui II* disclosure were imposed because the person concerned could not, in fairness, be required to rely on the opposing party (the Minister) to determine the information that person should have. Before the Special Advocate regime, judges alone decided what information to release, but further disclosure was sometimes made after the Special Advocates became involved.

Bill C-51's proposals would erode the delicate balance struck by further limiting the meaningful role Special Advocates play in representing an individual subject to secret proceedings. The proposed amendments to *IRPA* would gut the Special Advocate regime, imposing a system much like that in place before the Supreme Court's decisions in *Charkaoui I* and *Charkaoui II*.

The major change to the disclosure regime in Bill C-51 is at section 57. Proposed *IRPA* section 83(1)(c.1) would allow judges to relieve the Minister of the requirement to disclose "a copy of information" disclosed to the judge to the Special Advocate, where "the information does not enable the permanent resident or foreign national to be reasonably informed of the case made by the Minister". This would reverse the onus on the Minister to provide everything to the Special Advocate (except, in very narrow circumstances, where disclosure even to the Special Advocates would not be permissible under some pre-existing form of privilege or because it would be injurious to national security or endanger someone) to instead allow the Minister to ask to disclose *only* what in the Minister's view "reasonably informs" the person concerned of the allegations. This exemption is not linked to national security concerns, but left to the Minister to determine relevance of the information to the person concerned. Under *IRPA* section 77(2), the Minister is already required to file a public summary which "reasonably informs" the person with the Court.

This suggests that the Minister must only disclose to the Special Advocate any information that would "reasonably inform" the person concerned. Rather than disclosing almost everything to be scrutinized by the Special Advocate, the Minister may exempt information that the Minister believes is not necessary for the person to be "reasonably informed".

Another more legitimate reason for the Minister to not disclose something to the Special Advocate would be if disclosure, even to the Special Advocate, was shown to be injurious to national security. As discussed, such an exemption is redundant, given the existing mechanisms to deal with this issue.

#### RECOMMENDATION:

21. The CBA recommends that the proposed IRPA section 83(1)(c.1) be deleted.

## **B. Fair Appeals for All Parties**

Bill C-51 would allow further appeals under *IRPA* that only benefit the Minister. Asymmetrical access to appeals and judicial review is unfair, further skewing the parties' positions in a process already heavily balanced against the person subject to non-disclosure.

## Lifting the leave requirement

Applicants seeking to challenge an immigration decision at the Federal Court cannot apply directly for judicial review: under section 72, they must seek leave of the Court, and prove their case is sufficiently serious. This requirement was found constitutional by the Federal Court of Appeal in *Bains v. Canada*:

the requirement of leave does not deny ... access to the Court. *The right to apply for leave is itself a right of access to the Court* and, in our opinion, the requirement that leave be obtained before an appeal or application for judicial review may proceed does not impair rights...<sup>54</sup>

Bill C-51 would remove the requirement to seek leave for the Minister only. The Bill would make the leave requirement "subject to s. 86.1". Proposed *IRPA* section 86.1 (in section 60 of the Bill) would give the Minister power to apply for judicial review *without* applying for leave, to challenge the refusal of an application for non-disclosure by the Immigration Division or Immigration Appeal Division under *IRPA* section 86. This will arise where the Minister has applied to not disclose information in proceedings before the Immigration Division or Immigration Appeal Division. If the Member at those proceedings refuses all or part of the application for non-disclosure under *IRPA* section 86, the Minister could use the proposed section 86.1 to seek relief from the Federal Court without first obtaining leave.

There is little case law on *IRPA* section 86, and nothing to suggest the Minister requires a special and urgent route of review. Should the Minister need to halt an Immigration Division case, there are already two options:

Bains v. Canada (Minister of Employment and Immigration), [1990] F.C.J. No. 457 (FCA). See also Krishnapillai v. Canada, [2002] 3 FCR 74, 2001 FCA 378.

- (1) request a stay or postponement from the Division and, if it is not granted, they can seek a stay from Federal Court pending leave;
- (2) withdraw the information, under protest, and if they are unsuccessful at the Immigration Division, raise the issue at judicial review.

The section proposed in Bill C-51 would impede the fairness of the process by giving the Minister preferential treatment, suggesting in advance that the Minister's intervention will be sufficiently serious such that it should not be screened at the leave stage.

#### **RECOMMENDATION:**

22. The CBA recommends deleting changes to *IRPA* section 72 from Bill C-51.

### Lifting the "certified question" requirement

Proposed amendments to *IRPA* section 74(d) (section 53 of the Bill) and the addition of *IRPA* sections 79.1, 82.31 and 87.01 (section 55, 56 and 60 of the Bill, respectively), would also tip the balance of fairness of the process in favour of the Minister. For the Minister only, these provisions would permit an appeal to the Federal Court of Appeal from a decision of the Federal Court requiring disclosure, without having to seek a certified question from the lower court. The Minister could appeal from an interlocutory decision of the lower court which is currently barred under normal circumstances.<sup>55</sup>

#### **RECOMMENDATION:**

23. The CBA recommends deleting proposed amendments to *IRPA* section 74(d) and omitting proposed *IRPA* sections 79.1, 82.31 and 87.01.

# VIII. PROTECTING THE WORK OF CHARITIES AND NOT-FOR-PROFITS

At first glance, it might seem that there is little new in Bill C-51 from the perspective of charities and not-for-profit organizations. Previous CBA submissions<sup>56</sup> have outlined concerns about the interplay between Canada's anti-terrorism laws and the broad impact of audit and sanction capabilities of Canada Revenue Agency (CRA) for charities operating

The requirement for a certified question was brought in by amendments in the 1990s. It was discussed in detail in *Huynh v. Canada*, (Citizenship and Immigration), 2010 83248 (IRB) and has been more recently affirmed in *Huntley v. Canada* [2012] 3 F.C.R. 118.

Submission on the *Three Year Review of the Anti-terrorism Act* (Ottawa: CBA 2005), online: www.cba.org/cba/submissions/pdf/05-28-eng.pdf.

in conflict zones, specifically around their ability to demonstrate effective control over charitable assets and programs to avoid placing the organizations, and their directors, officers, employees and volunteers at risk.

The sector has already seen instances where only a suspicion of ties to terrorist organizations or activities has escalated from allegations to "fact", without an opportunity for the impacted organizations to properly defend themselves. These claims have serious consequences, not only for the organization, but for its board of directors, officers, employees, volunteers, and even members and their families, for their capacity to carry out charitable activities and for personal security. These concerns are heightened by Bill C-51.

# A. Security of Canada Information Sharing Act

The definition of an "activity that undermines the security of Canada" is extremely broad despite exemptions offered to narrow the scope of the definition.

For example, under section 2(i), there is room for interpretation of what will be considered an "activity" and be seen to "undermine the security of another state", especially with the constantly changing landscape of international conflicts and the unstable nature of many states. The government might use the breadth of the definition of "activity" in Bill C-51 to target groups simply for advancing positions that do not conform to its policies and priorities. This has already played out in Canada in recent years, reflected in statements by Cabinet ministers about environmental or aboriginal organizations, particularly those suspected of being funded by foreign groups opposed to government policies. <sup>57</sup> As currently worded, the section could unduly restrict the ability of charities and not-forprofits to know in advance what sort of activities or programs may trigger the new information sharing provisions.

Also of concern to employees and volunteers of charities and not-for-profits working in the international context, particularly in conflict zones, is that information sharing may be initiated on a government institution's own initiative, or on the request of the recipient institution. SCISA permits a recipient institution to use the information or further disclose it to any person, for any purpose. Once the information is shared, any controls governing the government institution that collected the information in the first instance no longer

<sup>57</sup> 

apply. No civil proceedings lie against any person for disclosure in good faith of information under the Act.

As discussed earlier in this submission, the list of government institutions between which information can be shared is lengthy. For charities and not-for-profits, the most concerning sharing would be between CRA, the RCMP, CSIS, CBSA and the Department of Public Safety and Emergency Preparedness. Consequential amendments to the *Income Tax Act (ITA)* confirm that CRA can share publicly accessible charity information and arguably broaden the personal taxpayer information that can be shared and with whom. The amendments will allow CRA to share information that falls under the broadly defined category of "taxpayer information", as opposed to the more narrowly defined "designated taxpayer information" that it can currently share with CSIS, the RCMP, and the Financial Transactions and Reports Analysis Centre of Canada, under the *ITA*.

## **B. Secure Air Travel Act**

The no-fly lists concerns expressed earlier are of particular concern to employees and volunteers of charities and not-for- profits working in conflict zones. The proposed list (including given name, surname, known alias, date of birth and gender of the person) omits other identifying information that would assist in differentiating individuals.

The proposal for regular review of the list and an effective administrative appeal process for individuals wrongly listed is little comfort given the seriousness of being included on list in the first place.

## C. New Terrorism Offence

Part 3 of Bill C-51 would add a new terrorism-related offence of "advocating or promoting the commission of terrorism offences in general".

Without clear definitions on the application of this broadly defined offence, the work of charities and not-for-profits carrying out activities in conflict zones would need to be carefully reviewed to assess any risk to the organization and its reputation of unintentionally becoming involved in this offence and, whether any risk can be reasonably managed. For example, a charity's fundraising activities may be a primary source of risk with articles, blogs, tweets, posters, pamphlets, and online videos all being subject to scrutiny as possibly "advocating or promoting the commission of a terrorism offence in general." Bill C-51 would likely confront *Charter* and other challenges, including those

related to its impact on charities and not-for-profits that express religious and ideological ideals and engage in corresponding activities.

## IX. CONCLUSION

The CBA supports government efforts to enhance the safety and security of Canadians that are necessary, proportionate and accompanied by adequate safeguards against abuse. Promising public safety as an exchange for sacrificing individual liberties and democratic safeguards is not, in our view, justifiable. Both are essential and complementary in a free and democratic society.

The CBA has recommended several amendments to Bill C-51, with a view to achieving an appropriate balance.

When extraordinary powers of surveillance, intelligence-gathering and sharing, preventive arrest and detention are contemplated, shown to be necessary and then implemented, equally extraordinary mechanisms of oversight and after-the-fact review must also be in place to provide the necessary balance to those initiatives.

The CBA believes that Bill C-51 must be amended to create specific and general sunset clauses to ensure that the most extreme extensions of state power are the subject of sober and objective review within three or five years. Further, the Bill must contain a mechanism for contemporaneous oversight and rigorous review of the CSIS activities it contemplates.

For Bill C-51 to be a meaningful success, Canadians must not only feel safer but must in fact be safer – and this reality must be accompanied by the well founded and secure belief that Canada remains a democracy that leads the way internationally in scrupulously protecting privacy rights and civil liberties.

## X. SUMMARY OF RECOMMENDATIONS

- 1. The CBA recommends that *SCISA* include effective mechanisms to enforce the principles outlined in section 4.
- 2. The CBA recommends the scope of activities subject to information sharing under *SCISA* be narrowed, and that the exemption in section 2 of *SCISA* be expanded to specifically include unlawful protests that do not represent a genuine threat to national security.
- 3. The CBA recommends clarifying the interaction of the Privacy Act and the proposed *SCISA*.
- 4. The CBA recommends that section 6 of *SCISA* be narrowed to not allow disclosure of information to the private sector and foreign governments.
- 5. The CBA recommends that *SCISA* include safeguards to ensure that any shared information is reliable.
- The CBA recommends that SCISA be amended to provide effective oversight, including regular Parliamentary review of its effects and operations.
- 7. The CBA recommends:
  - providing an objectively discernible basis for additions to and removals from the no-fly list,
  - curtailing warrantless search powers, and
  - adding effective safeguards for those wrongly placed on the list, including a process for expeditious removal.
- 8. The CBA recommends that the proposed section 83.221 be deleted from Bill C-51.
- 9. The CBA recommends that the definition of "terrorist propaganda" be limited to material that counsels the commission of a terrorist offence or that instructs the commission of a terrorist offence.
- 10. The CBA recommends the proposed deletion orders for "terrorist propaganda" include a mental fault requirement, and defences to exclude legitimate public interest, education or religious discussion activities.

- 11. The CBA recommends allowing judges to appoint *amicus curiae* to address appeals of the proposed deletion orders.
- 12. The CBA recommends that the consequential amendment to the customs tariff be deleted.
- 13. The CBA recommends that Bill C-51 retain existing legal thresholds for preventive detention and permissible periods for detention, and include a sunset clause.
- 14. The CBA recommends that, instead of introducing a new regime for control orders, the current section 810.01(1) be retained, and amended if required to better address terrorism offences.
- 15. The CBA recommends the creation of an Office of the National Security Advisor, to act as an expert review body with resources and a mandate to review *all* national security activity, and to ensure effective information sharing and cooperation between CSIS and other security agencies, including the RCMP.
- 16. The CBA recommends amending section 12.2 to prohibit CSIS from arbitrarily detaining an individual and to clarify that "bodily harm" includes psychological harm.
- 17. The CBA recommends that the judicial warrant provisions in sections 12.1(3) and 21.1 of Bill C-51 be amended to ensure that they align with the fundamental role of Canada's judiciary in upholding the Rule of Law and Canada's constitutional guarantees.
- 18. In addition to the creation of an Office of the National Security Advisor, above, the CBA also recommends the creation of a Parliamentary review committee with access to secret information.
- 19. The CBA recommends that if CSIS mandate is expanded to engage in kinetic operations, the agency be subject to regular reporting requirements as to the nature and number of those operations, perhaps to the expert review body recommended above, whether pursuant to section 12.1 or to warrants under section 21.1.
- 20. The CBA recommends that Bill C-51 be brought back to Parliament for rigorous review after three or five years.

- 21. The CBA recommends that the proposed IRPA section 83(1)(c.1) be deleted.
- 22. The CBA recommends deleting changes to *IRPA* section 72 from Bill C-51.
- 23. The CBA recommends deleting proposed amendments to *IRPA* section 74(d) and omitting proposed *IRPA* sections 79.1, 82.31 and 87.01.