THE CANADIAN BAR ASSOCIATION

L'ASSOCIATION DU BARREAU CANADIEN

# Our Security, Our Rights: National Security Green Paper, 2016

**CANADIAN BAR ASSOCIATION**

**December 2016**

500-865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
**tel/tél** : 613.237.2925 | **toll free/sans frais** : 1.800.267.8860 | **fax/téléc** : 613.237.0185 | info@cba.org | **www.cba.org**

## 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 Criminal Justice, Immigration Law, Charities and Not-for-Profit Law, and Privacy and Access Law Sections, and with assistance from the Legislation and Law Reform Directorate at the CBA 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

## Our Security, Our Rights: National Security Green Paper, 2016

# Our Security, Our Rights: National Security Green Paper, 2016

## I. INTRODUCTION

The Canadian Bar Association appreciates the opportunity to participate in the Public Safety and Justice Ministers' study of national security in Canada. The CBA is a national association of over 36,000 members, including lawyers, notaries, academics and law students, with a mandate to seek improvements in the law and the administration of justice. We have offered our views and expertise at many stages in the development and critique of Canada's national security and anti-terrorism regime in the past[1] and remain committed to doing so going forward.

The Ministers outline the federal government's dual responsibility in an opening message to the Green Paper. The CBA agrees that protecting the safety and security of Canadians, and preserving Canadians' constitutional values are equally fundamental responsibilities of the federal government. We commend the Ministers' clear commitment to opening up this discussion so that all members of the Canadian public can participate and contribute.

We note, though, that the Green Paper seems unbalanced in its presentation of these two equal and primary considerations. Examples can be powerful and persuasive advocacy tools. Unfortunately, the scenarios in the Green Paper seem to favour implementation of the most controversial sections of Bill C-51, despite the government's commitment to carefully reconsider that Bill. Most of the illustrations and examples throughout the Green Paper and Backgrounder concern security threats or criminal activities, asking whether the public sees various proposals as an appropriate state response to those threats or activities. In contrast, readers are given no competing illustrations of how the proposed legislation might unnecessarily curtail their civil rights.

---

1 For a few examples, see our submissions on *Bill C-36, Anti-Terrorism Act* (Ottawa: CBA, 2001), *Three Year Review of the Anti-Terrorism Act* (Ottawa: CBA, 2005), *Policy Review of the Commission of Inquiry in relation to Maher Arar* (Ottawa: CBA, 2005) and *Bill C-51, Anti-Terrorism Act, 2015* (Ottawa: CBA, 2015).

For meaningful consultation, those being consulted must be equipped to make *informed* choices. In our view, the Green Paper does not give Canadians a balanced perspective to consider the potentially negative impact that excessive or unbalanced state powers might have on individual rights and freedoms. The decision to frame this important consultation about national security in this way should, at a minimum, be considered in evaluating feedback provided by Canadians.

## II. ACCOUNTABILITY

Robust accountability mechanisms are crucial to both the legitimacy and the efficacy of our national security agencies. Accountability has been a recurring theme in several studies and commissions on national security issues in Canada, even before the MacDonald Commission report in 1981. The reports by the Air India Commission of Inquiry (2010) and the Arar Commission (2006) raised similar concerns, as have academics and judicial decisions. The legitimacy of national security agencies is undermined by the conduct reviewed by each of those commissions, and accountability mechanisms ensure that conduct is eventually exposed and appropriately addressed.

Public confidence that accountability mechanisms are effective is critical to public confidence in our national security agencies, in particular for communities whose members are more frequently subjects of investigation by state agencies. The confidence of those communities in the legitimacy and accountability of national security agencies is also critical to the agencies' efficacy, as a perception that the agencies are unaccountable undermines both community confidence in and cooperation with their work.

The CBA has had the opportunity to review the commentary by Professors Kent Roach and Craig Forcese in response to the Green Paper, and we agree with many of their observations on this topic. First, there must be robust expert review at the agency level, including the Royal Canadian Mounted Police (RCMP) Complaints Commissioner, Security Intelligence Review Committee (SIRC) and the Communications Security Establishment Canada (CSEC) Commissioner. There are legitimate concerns about the scope of the mandate of some of the review bodies and those for CSEC and the RCMP are well described by Professors Roach and Forcese. In basic terms, the CBA supports a mandate for the review bodies that is at least as broad as the mandate of the agency under review, with the tools necessary to review any of the activities of the agency in question.

Certain agencies, like the Canada Border Services Agency (CBSA), do not have independent review bodies at all, and the CBA continues to call for independent review of those agencies. Cooperation between review bodies should be facilitated in particular where the agencies are working jointly or sharing information.

Second, we believe there should be higher level review of the national security infrastructure as a whole. This would be achieved by adding two mechanisms to the current oversight and review framework. One is a national security committee of Parliamentarians, and the CBA has expressed our support for creating this committee in a submission on Bill C-22, currently before Parliament.[2] The role of a Parliamentary committee would be higher-level examination of policy and the functioning and framework of the national security infrastructure as a whole. A properly resourced office would provide a necessary level of expertise and institutional memory.

The other mechanism is what Professors Roach and Forcese call a 'National Security and Intelligence Review and Complaints Commission' or 'Super-SIRC'. The CBA also supports the creation of a commission, largely for the reasons set out in the professors' paper. The ability to review the work of agencies in a broader context is crucial, given the current realities of broad information-sharing and coordinated action by several agencies. For many of the same reasons that several agencies currently answer to the Minister of Public Safety, there should be a comprehensive review mechanism for the national security infrastructure as a whole. While often day-to-day complaints and concerns could be primarily addressed by individual agency review bodies, systemic issues should be addressed in a coherent and consistent way across agencies. The expertise developed by the commission would allow for more effective and reliable review.

**RECOMMENDATION**

1. **The CBA recommends that agency review bodies have a mandate at least as broad as the agency's mandate, with tools to review any of the agency's activities.**
2. **The CBA recommends the creation of:**
    - **a national security committee of Parliamentarians with a mandate to examine national policies and the overall functioning and framework of the national security infrastructure, and**

2 See, CBA submission on *Bill C-22, Committee of Parliamentarians Act* (Ottawa: CBA, 2016).

- **an overarching national security review and complaints commission, resourced to act as a comprehensive review mechanism to address systemic issues in a consistent and coherent way across national security agencies.**

## A. Role of the Courts

The courts have an important role to play in balancing the rights and freedoms of individuals with the legitimate interests of the state. Requiring judicial warrants and authorizations for law enforcement to undertake certain activities has provided an effective mechanism. We have expressed concerns, however, about expanding the role of judges in legitimizing activities undertaken in secret.[3] The CBA expressed particular concerns about parts of the *Anti-Terrorism Act, 2015* that allow judges to authorize breaches of the *Charter* in secret hearings.[4] These mechanisms, aside from being constitutionally vulnerable, risk undermining public confidence in the courts themselves if judges are seen as complicit with security agencies rather than transparent, neutral arbiters safeguarding the rule of law. As a general principle, courts should function in an open, adversarial system to the furthest extent possible. To the extent that secrecy is at times required, other mechanisms such as special advocates can be put into place to ensure a strong defence of the rights and interests of individual citizens.

## B. Transparency

A primary concern in developing national security law is around laws applied under the cloak of secrecy. The CBA recognizes legitimate grounds to maintain privilege around certain types of deliberations and advice, whether in cabinet or advice provided in a solicitor-client context, as well as the rationale for secrecy surrounding certain types of operational information, but it is less clear why interpretations of the law being applied in secret should not be made public. The development of a body of secret law is contrary to democratic processes and undermines confidence in the national security framework. In the context of operational secrecy, the legal basis that grounds government actions should be public to permit discussion of the legal framework itself.

The 2015-2016 SIRC *Annual Report* provides an example of this issue, undertaking for the first time a review of the use of bulk datasets by CSIS. The report outlines some of the legal framework within which CSIS understands itself to be operating. It distinguishes between

---

3 http://www.sirc-csars.gc.ca/anrran/2015-2016/index-eng.html

4 *Supra* note 1 at 32.

'referential' and 'non-referential' datasets, and finds the former not to be 'collected' under section 12 and so not subject to restrictions on collection.[5] We see little reason why this legal framework, operationalized by national security agencies in secret, could or should not be made public to permit discussion of the legal framework for the agencies' operations. Unlike other areas of law where the effects of interpretations of law within agencies can be observed by the public, in the context of secrecy those effects may never be known or publicly scrutinized. Presumably, the legal interpretations surrounding the bulk dataset framework have been in place for years, and SIRC has not inquired into the programs until now. In our view, the default should be for agencies acting in secret to make the legal framework within which they understand themselves to be working transparent and subject to public scrutiny.

## III. PREVENTION

Perhaps the most effective strategy to address national security is to prevent radicalization in the first place, rather than dealing with its consequences. The CBA supports the Green Paper's call for working with communities to identify and support individuals at risk of radicalization.

While the CBA acknowledges the role that law enforcement must play in prevention, we caution against excessive reliance on law enforcement and a criminalized response to this problem. As the Green Paper notes, radical ideology is not a crime – only when violence is adopted in furtherance of that ideology is a crime committed. Additionally, marginalized communities may already distrust law enforcement and that can undermine the overall effectiveness of law enforcement efforts. Available *Criminal Code* tools like peace bonds and recognizances with conditions should not be overused to respond to this issue. Finally, the CBA supports federal government funding for research to develop a sufficient evidence base to make informed policy decisions in this area. We suggest that funding be made available to a wide range of stakeholders including academics and community organizations to encourage a participatory or partnership approach to research.

**RECOMMENDATION**

3. **The CBA recommends that research funding to develop an evidence base for informed policy decisions to prevent radicalization be extended to**

5 *In the Matter of an Application by XXX for Warrants Pursuant to ss.12 and 21 of the Canadian Security Intelligence Act* 2016 FC 1105 shows another example, where the agency was applying legal interpretations of 'associated data' to allow for indefinite retention of information gathered under warrants where the contents of communications were to have been retained for limited periods.

**academics, community organizations and others to encourage a participatory or partnership approach to research in this area.**

## IV. THREAT REDUCTION

One of the most concerning changes from Bill C-51 is the 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 fundamentally transforms the agency's role. The CBA continues to be concerned about the scope of the additional mandate and the lack of accountability and oversight commensurate with the agency's new role. In our submission on Bill C-51 we said:

> In particular, proposed section 12.1(3) combined with the warrant provisions in section 21.1 is 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*.

The wording of proposed sections 12.1(3) and 21.1 is ambiguous at best, and may not accurately reflect the drafters' intent. One interpretation is that they provide for judicial warrants to authorize the violation of any *Charter* rights. While senior government officials have assured us that this is not the intent, the fact that many legal experts read the relevant sections in this way is a sufficient concern that the language should be clarified.

Judicial warrants for search and seizure are intended to prevent, not authorize, *Charter* violations. 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, 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*.

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. The CBA believes that this invitation to *Charter*

violations is unlikely to be justified under section 1 or to be interpreted as being 'prescribed by law'.

While the government has 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. If it does not, CSIS may be empowered to seek authorization to conduct psychological torture (contrary to section 12 of the *Charter*).

**RECOMMENDATION**

4. **The CBA recommends that the judicial warrant provisions in sections 12.1(3) and 21.1 of Bill C-51 be amended so that CSIS warrants can never violate the *Charter*. The use of the section 21.1 warrant should only be used to justify action that would otherwise be contrary to Canadian law but not to justify any *Charter* violation.**
5. **The CBA recommends amending section 12.2 to prohibit CSIS from arbitrarily detaining an individual and to clarify that 'bodily harm' includes psychological harm.**

## V. DOMESTIC NATIONAL SECURITY INFORMATION SHARING

The *Security of Canada Information Sharing Act* (*SCISA*) has significantly expanded information sharing, including personal information, without precise definitions, basic privacy protections or clear limitations on the purpose for intra-governmental sharing of personal information.

Consistent with the CBA's previous position on Bill C-51, we emphasize that there must be appropriate respect for both 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. While some helpful changes were made to *SCISA* before its final passage into law, the statute still causes concern on several fronts.

## A. Guidance without Oversight

Helpfully, section 4 of *SCISA* proposes a number of 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, but to be meaningful and effective *SCISA* must include a mechanism to enforce them.

The current proposals in Bill C-22, *National Security and Intelligence Committee of Parliamentarians Act* would allow that committee to review 'any activity carried out by a department that relates to national security or intelligence.'[6] If created, this committee might be an appropriate body to ensure that information sharing by government institutions under *SCISA* is carried out appropriately, not only under section 4, but the Act as a whole.

In addition, to better facilitate review of activities carried out under *SCISA* – whether by a Committee of Parliamentarians, another designated general oversight body or the Privacy Commissioner of Canada (OPC) – regulations should be introduced requiring institutions to keep a record of disclosures made under *SCISA*, as well as, for recipient institutions, records of subsequent use and disclosure of information received pursuant to *SCISA*.

**RECOMMENDATION**

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

6 Bill C-22, section 8(b).

7. **The CBA recommends that regulations be enacted under *SCISA* requiring records to be kept of disclosures made under *SCISA*, as well as records of subsequent use and disclosure of information received pursuant to *SCISA*.**

## B. Sharing with Institutions

Section 5(1) of *SCISA* permits disclosure among the 17 government institutions in Schedule 1 if:

> …the information is *relevant to the recipient institution's jurisdiction or responsibilities* under an Act of Parliament or another lawful authority in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption. [Emphasis added]

Mere relevance is a very low standard for what should be an exceptional sharing of information between departments. As others including the OPC have commented, a simple test of relevance to the recipient's mandate could allow unnecessary and overbroad sharing of information. A preferable threshold would combine relevance with an additional test of necessity to filling the receiving institution's statutory responsibilities relating to national security. As the OPC has pointed out, the standard under the *Canadian Security Intelligence Service Act* to permit CSIS to collect information is where collection is 'strictly necessary'. This may also be an appropriate and symmetrical standard under *SCISA*.

In the same vein, several institutions in Schedule 3 to *SCISA* have broad mandates that go well beyond national security. At a minimum, information should be shared under section 5 only if clearly relevant to a specific statutory authority that relates to national security. It would help if Schedule 3 listed not only the names of potential recipient institutions and their designated heads, but also the specific sections of the statutes supervised or implemented by those institutions that might relate to national security concerns. Greater specificity would assist both disclosing and receiving institutions, as well as any oversight body in assessing whether disclosure to another institution might be appropriate.

As an overarching comment, the CBA is concerned about how the restrictions in section 5 would work in practice. Practically, before disclosing information to another Schedule 3 institution, the disclosing institution would have to determine the relevance of that information to the recipient institution's jurisdiction or responsibilities. While references to specific statutory provisions that relate to national security (as recommended above) have already been added to Schedule 3 for each listed institution, section 5 still places an implicit burden on a disclosing institution to be sufficiently familiar with a recipient institution's mandate to

determine whether any given information will be relevant to its fulfillment. If the test for disclosure is strengthened to permit disclosure only where strictly necessary, as we also recommend, the disclosing institution would be faced with an even more difficult assessment.

It may be preferable for all information of potential value to national security to be disclosed to a single, centralized expert authority for distribution, as relevant and strictly necessary, to the institutions listed in Schedule 3.

**RECOMMENDATION**

8. **The CBA recommends that section 5(1) be amended to allow a government institution to disclose information to a designated recipient institution only where the information is both relevant to the recipient institution's mandate respecting national security and "strictly necessary" to fulfill that mandate.**

9. **The CBA recommends that Schedule 3 to *SCISA* be amended to list not only the names of potential recipient institutions and their designated heads, but also the specific sections of the statutes supervised or implemented by those institutions that may conceivably relate to national security concerns.**

## C. Further Disclosures

A remaining concern with *SCISA* is the lack of restrictions around subsequent use and disclosure of information disclosed to an institution under section 5. While this was amended before Bill C-51 was passed, we remain concerned that it places insufficient restrictions on subsequent use and disclosure of information received under that section. The provision seems to allow for the subsequent disclosure by a recipient institution to other, non-designated government institutions, to individuals, to foreign governments, or to the private sector.

The CBA is particularly concerned about subsequent use and further disclosures where information has been obtained by a disclosing institution through the exercise of extraordinary powers, such as powers to compel production of information or enter premises. It would be inappropriate for an institution that lacked similar powers to make further use of information disclosed to it under section 5(1). Otherwise the receiving institution would benefit from investigation and enforcement powers not conferred on it by Parliament. *SCISA* should not allow receiving institutions to obtain indirectly that which they could not obtain directly.

Section 6 says that subsequent disclosures are neither authorized nor prohibited by *SCISA*, but must be done in accordance with the law, including any legal requirements, restrictions and prohibitions. It is unclear what 'in accordance with the law' means here, but it could reference the *Privacy Act* and the laws supervised or implemented by the recipient institutions.

About the latter, to the extent that the laws supervised or implemented by the designated potential recipient institutions would provide few restrictions on use or disclosure, this would create a loophole that could allow significant and inappropriate 'purpose creep' – including potential disclosure to third parties. In the CBA's view, the information sharing between government institutions contemplated by *SCISA* should be seen as an extraordinary measure, designed to fulfil an explicit, narrow purpose. It is incumbent on the federal government to explicitly restrict subsequent use and disclosure of that information. It is not enough to leave further disclosures to be governed by existing, sector-specific statutes that may govern the activities of designated potential recipient institutions.

On the *Privacy Act*, 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. That goal is different from the purpose in the *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* as a result of section 5(1) of *SCISA*, the *Privacy Act* explicitly allows disclosure authorized by *any other Act of Parliament,*[7] 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 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.

---

7 *Privacy Act*, RSC 1985, c. P-21, section 8(2)(b).

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'. It is unclear that personal information shared under *SCISA* would continue to be covered by the remaining protections under the *Privacy Act*.

**RECOMMENDATION**

10. **The CBA recommends that section 6 of *SCISA* be narrowed so as to prohibit subsequent disclosure of information to the private sector and foreign governments and to limit subsequent use by recipient institutions for the purpose of ensuring national security.**
11. **The CBA recommends clarifying the interaction of the *Privacy Act* and the proposed *SCISA*.**

## D. Limited Checks and Balances

There are few effective checks and balances on information sharing 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.[8] 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 in Syria. The Arar Commission stressed the importance of precautions to ensure that 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 relevance requirement appears to limit the scope of information sharing, the broad definition of 'activities that undermine the security of Canada' would mean almost

8 Commissioner Dennis O'Connor, *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (Ottawa: 2006).

everything is relevant. The expression 'jurisdiction or responsibilities' is also so broad it could encompass almost anything.[9]

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**

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

## VI. PASSENGER PROTECT PROGRAM

In 2015, the CBA supported 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. 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 on the list must be subject to direct Ministerial or Parliamentary review. A process for removing a name from the list must be expeditious and effective, given the potential for error and the significant detrimental consequences of being included erroneously.[10]

We highlighted several concerns about this aspect of Bill C-51, which remain applicable:

- the likelihood of false positive matches, given that only basic information about individuals will be on the no-fly list.

---

9 Craig Forcese and Kent Roach, *Bill C-51 Backgrounder # 3: Sharing Information and Lost Lessons from the Maher Arar Experience* at 31. Available at www.antiterrorlaw.ca.

10 CBA submission on *Bill C-51, Anti-Terrorism Act 2015* (Ottawa: CBA, 2015).

- criteria for placing a person on the no-fly list that are unclear.
- what it takes to be put on the list not objectively discernible, nor information that is relied on tested by responsible authorities and found to be reliable.
- *SATA* could interfere with other civil liberties as well, including introducing powers to search computers and mobile devices without warrant, and without oversight.[11]
- Lack of safeguards for those wrongly placed on the list.
- People denied travel may make submissions, but not to access information as to why they were put on the list.
- A less than ineffective appeal process.[12]

**RECOMMENDATION**

**13. The CBA recommends that the federal government:**

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

## VII. *CRIMINAL CODE* TERRORISM MEASURES

**Are the thresholds for obtaining the recognizance with conditions and terrorism peace bond appropriate?**

The *Anti-terrorism Act, 2015* lowered the threshold to obtain a recognizance with conditions to where a peace officer believes on reasonable grounds that a terrorist activity 'may' be carried out. Previously, the law required belief on reasonable grounds that a terrorist activity 'will' be carried out. The 2015 amendments also replaced a requirement that a recognizance is 'necessary to prevent' the carrying out of a terrorist activity with 'is likely to prevent'.

The CBA recommended retaining the more stringent thresholds for preventive detention and permissible periods for detention in 2015, and continues to believe the lower thresholds are problematic. The Green Paper suggests that the requirement to obtain consent of the Attorney General before making an application for a recognizance acts as a procedural safeguard. We

11 See, *R. v. Fearon* 2014 SCC 77 at para 51.

12 *Supra,* note 8 at 19-20.

believe this is inadequate and provides little protection. While we respect the work of prosecutors, we do not support the proposal that the Crown should exercise appropriate discretion to justify a liberty-restricting regime.

A lower threshold may upset what would otherwise be an appropriate balance between an individual's liberty interests and the security needs of society. Terrorism offences can capture a wide range of conduct, from actually committing or planning a terrorist attack to being reckless in advocating or promoting a terrorist offence. Other offences involve financing or otherwise supporting a terrorist organization where the list of those organizations is at the discretion of the Governor in Council. Again, a 'may commit' standard could be problematic. This is significant not just for the required grounds of the recognizance itself, but the increased penalties for breach of up to four years' imprisonment.

Other amendments to terrorism recognizance provisions increased the time a person may spend in custody before a court hearing on the recognizance to seven days. While reviews by a judge are required at the initial 24 hour point, and then subsequent 48 hour marks, further restricting liberty interests while at the same time reducing the threshold for detention has the potential to attract scrutiny under section 7 of the *Charter*. Increasing the potential sentence to four years for breach of a recognizance while simultaneously lowering the threshold for obtaining a recognizance equally raises potential *Charter* issues.

Finally, there is no mandatory review mechanism for the recognizance provisions. A mandatory review of conditions imposed during the term of the recognizance would help to balance the competing interests at stake and mitigate potential deprivation of other *Charter*-protected rights. In addition, the consequences for failure to enter into the recognizance at the court's direction could result in incarceration for up to 12 months, compelling the individual to agree to any conditions to avoid custody. This is especially significant given the lower standard now in force. Any reduction in the threshold for detention should be counter-balanced with increased procedural protections.

The previous thresholds provided an adequate basis for judges to balance societal protection with individual liberty. Without empirical evidence that the previous thresholds were problematic, the CBA sees no justification for further incursion into the rights of uncharged individuals. We suggest a return to the previous legal thresholds and the application of a sunset clause for these provisions. In the alternative, should new amendments not return to the previous thresholds, we recommend additional procedural safeguards.

**Advocating and promoting the commission of terrorism offences in general is a variation of the existing offence of counseling. Would it be useful to clarify the advocacy offence so that it more clearly resembles counseling?**

In 2015, the CBA recommended the deletion of section 83.221 from Bill C-51, and we continue to recommend that the advocacy offence be deleted altogether. It is overbroad, vague and contrary to the core principle that the criminal law must be certain and definitive. It lacks a legal definition of the term 'advocates'" or 'promotes', and applies to all 'statements' and to 'terrorism offences in general', rather than simply terrorist activity. When laws are unclear, judges must struggle to fill in the substance of the offence within the context of costly and lengthy litigation.

These provisions invite *Charter* scrutiny under section 2(b), freedom of expression, despite the suggestion that they go beyond mere expression. Incorporating a recklessness standard into the offence, which is not included for the counselling offence, may also invite constitutional scrutiny. The existing extensive case law for 'counselling an offence' could be helpful in addressing these concerns. To distinguish terrorism offences from general counselling provisions under the *Criminal Code* creates the possibility of disproportionate application especially for groups that tend to be frequently associated with terrorism.

We suggest rather than altering or clarifying the offence, section 22 of the *Criminal Code* prohibiting counselling an offence should be interpreted as adequately and fairly addressing the objects of the advocacy offence.

**Should the part of the definition of terrorist propaganda referring to the advocacy or promotion of terrorism offences in general be removed from the definition?**

We support deletion orders for terrorist propaganda in principle, but the definition of 'terrorist propaganda' is overly broad and relies on the same language as the 'advocating terrorism' offence. It operates without a mental fault requirement, so a deletion order may be imposed even if the author had no intent or awareness that the material was 'terrorist propaganda'.

Further, the definition does not include public interest, education or religious discussion offences. Academic or political commentary only indirectly connected with anything that might be called violent could be considered 'terrorist propaganda' and subject to a deletion order. This type of censorship is harmful to Canada's democracy and likely to elicit constitutional scrutiny.

The CBA recommends that the definition should be limited to material that counsels the commission of a terrorist offence or that instructs the commission of a terrorist offence. The criteria for a deletion order should include a mental fault requirement, and defences should be provided to exclude legitimate public interest, education or religious discussion activities.

**RECOMMENDATION**

14. **The CBA recommends a return to the previous legal thresholds for recognizance with conditions and terrorism peace bond, and the application of a sunset clause for these provisions. In the alternative, we recommend additional procedural safeguards.**
15. **The CBA recommends deleting the advocacy offence under section 83.221 and that section 22 of the *Criminal Code* prohibiting counselling an offence be interpreted as adequately and fairly addressing the objects of that offence.**
16. **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.**
17. **The CBA recommends that the criteria for a deletion order should include a mental fault requirement, and defences should be provided to exclude legitimate public interest, education or religious discussion activities.**

## VIII. PROCEDURES FOR LISTING TERRORIST ENTITIES

The Green Paper identifies three existing methods for listing terrorist entities in Canada – two established under the *United Nations Act* and the third under the 2001 *Anti-terrorism Act* amendments to the *Criminal Code*. Listing an entity means freezing the known funds of the entity and additional *Criminal Code* sanctions for activities related to the listed entity.

In our view, the current listing regime lacks adequate safeguards to appropriately ensure both that Canadians are safe and that their fundamental rights are protected. It provides effective tools for law enforcement and regulatory investigators to carry out their functions, but can be too blunt an instrument for charitable organizations and their members to mount an effective defence against serious allegations.

The *Charities Registration (Security Information) Act* lacks any rigorous legal procedure, and permits the government to refuse to register or deregister a charity without that charity receiving full particulars of the allegations. This can expose historically legitimate vehicles for providing humanitarian aid in conflict zones to severe sanctions. Under section 6, a single judge has power to determine if disclosure of information implicating the suspected charity would compromise national security or endanger the safety of a person. That judge may also exclude the charity from knowing the allegations supporting deregistration, possibly including evidence not otherwise admissible in court. While we appreciate the national security rationale, this is not in keeping with fundamental principles of due process. The Act should, at a minimum, provide an appeal of the judge's determination so that another judge can assess the reasonableness of the initial determination, and balance national security concerns with depriving the impugned charity of appropriate due process.

While the Green Paper speaks to the issue of accountability in light of the "unique intelligence collection and enforcement powers to protect national security", it does not adequately recognize the impact of the 'terrorist' label on an organization and its members. The consequences that immediately follow the listing can effectively negate a response through available channels for appeal, and this is particularly true where full and frank disclosure is not provided.

The listing regime also fails to consider the personal consequences for individuals associated with listed entities, whether as a director, officer, member, donor or their family members. This is true for criminal sanctions, revoking registered charity status and labelling directors and senior management as 'ineligible individuals' under the *Income Tax Act*, loss of essential services (e.g. bank accounts), or fear for safety when, for example, there is a suggestion that a charity is not exercising due diligence to ensure that it and its staff, board members, officers, corporate members, donors, agents and other third parties acting on the charity's behalf were not directly or indirectly facilitating terrorist activities.

The question of what could be done to improve the efficiency of the listing processes could be balanced by also asking whether adequate safeguards against unproven allegations are in place. We suggest the government investigate means of ensuring those listed through the regime have the resources to respond effectively to allegations, whether financially or through a full and frank disclosure of the claims being made against the entity.

**RECOMMENDATION**

18. **The CBA recommends that the *Charities Registration (Security Information) Act* provide an appeal of the single judge's determination under section 6 to allow another judge to assess the reasonableness of the initial determination to balance national security concerns with the impact on the impugned charity.**

19. **The CBA recommends consideration be given to ensuring those listed have resources to respond effectively to allegations, whether it be financially or through a full and frank disclosure of claims against the entity.**

## IX. TERRORIST FINANCING

For several years, a focus of the federal government anti-terrorism and money laundering compliance efforts has been on Canada's registered charities. Charities generally attempt to comply with Canada's anti-terrorism legislation, but can find it practically challenging, as compliance often proves complex and costly. In addition, the state of Canada's anti-terrorism legislation means that Canada is potentially at odds with its responsibilities as a signatory to international treaties on human rights and international laws of war (such as the Geneva Conventions and their Additional Protocols).

Continuing dialogue with stakeholders in the charities and not-for-profit sector would strengthen cooperation between the government and that sector. Canadian registered charities often find Canada's anti-terrorism legislation overly broad and confusing. For example, section 83.03 of the *Criminal Code* makes it an offense to directly or indirectly collect property, provide or invite a person to provide or make available property or financial or other related services … for the purpose of facilitating or carrying out any terrorist activity, or for the purpose of benefiting any person who is facilitating or carrying out such an activity, or knowing that, in whole or part, they will be used by or will benefit a terrorist group. Section 83.19 makes it an offence to knowingly facilitate a terrorist activity. However, the *mens rea* element of the offence, i.e. 'knowingly', is rendered meaningless by paragraph 83.19(2) which states that a terrorist activity is in fact facilitated whether or not (a) the facilitator knows that a particular terrorist activity is facilitated; (b) any particular terrorist activity was foreseen or planned at the time it was facilitated; or (c) any terrorist activity was actually carried out.

This issue was raised during the Air India Commission of Inquiry. Commissioner Honourable John Major made the point that Canada's anti-terrorism legislation should not "unnecessarily impede the valuable activities of legitimate organizations…".[13]

Charities operating internationally often report that a lack of clear rules or guidelines from the federal government means they do not know exactly how to comply with Canada's anti-terrorism legislation. Lawyers cannot safely advise charities that adopting, implementing and complying with a comprehensive anti-terrorism policy that imposes due diligence on projects, partners and donors will be a sufficient defence to allegations of directly or indirectly facilitating terrorism.

**RECOMMENDATION**

**20. The CBA recommends that the federal government:**

- **amend section 83.19(2) of the *Criminal Code* on facilitation, to eliminate the strict liability element of the offence and require the Crown to prove criminal intent.**
- **create an exception for the delivery of humanitarian aid that incidentally supports a member of a terrorist group (for example, a charity that delivers medical supplies to a hospital that treated a member of a terrorist group would not be subject to prosecution).**
- **institute a clear *mens rea* requirement to the *Charities Registration (Security Information) Act*.**
- **amend the *Charities Registration (Security Information) Act* so the Federal Court judge to whom a certificate is referred shall not find the certificate to be reasonable where an applicant or registered charity establishes that it has exercised reasonable due diligence to avoid the improper use of its resources.**
- **amend the *Charities Registration (Security Information) Act* to allow an appeal to the Federal Court of Appeal of a decision by a Federal Court judge that a referred certificate is reasonable.**
- **develop Canadian guidelines for charities operating abroad or domestically so those charities can show due diligence in complying with anti-terrorism legislation.**

13 See Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 website at http://www.majorcomm.ca/en/reports/finalreport/volume5/ for the fifth Volume of the Report at 262.

## X. INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

The CBA appreciates the Green Paper's reconsideration of 'lawful access' (a term used to describe enhanced investigative powers for law enforcement), with the intent of avoiding problems of invalidity that occurred in the *Tse* and *Spencer* cases before the Supreme Court of Canada. We agree with several introductory statements in the Green Paper:

- most criminal activity now involves digital technology
- digital evidence is as important as physical evidence
- investigators must have digital capabilities
- law lags behind technological developments
- investigative capabilities have potential impacts on *Charter* rights
- key issues include access to subscriber information, intercept capability, encryption, and data retention

As the Green Paper notes, there have been multiple public consultations on lawful access but Canada's digital environment continues to change dramatically.[14] We suggest that meaningful, well informed consultation with Canadians in this area remains important.

To that end, we urge that enhanced investigative capabilities for law enforcement not be unduly conflated with national security or anti-terrorism initiatives. Any additional powers would likely be used by law enforcement in all manner of criminal investigations. Previous proposals for lawful access were framed first as linked to and essential to combat child pornography, and later, after some tragic deaths of young people, to address cyberbullying. Meaningful, well informed public consultation on enhanced investigative capabilities for law enforcement should frame those capabilities simply for what they are: additional police powers that may be needed to keep pace with technological advancements. This characterization allows the public to assess their potential value and their potential impact on privacy and *Charter* rights, without reacting emotionally to egregious criminal or terrorist activities.

Finally, we note that several unobjectionable lawful access provisions from Bill C-30, *Protecting Children from Internet Predators Act* in 2012 were included in Bill C-13, *Protecting Canadians from Online Crime Act*, many of which the CBA supported in 2014.

---

14 Backgrounder to the Green Paper at 56.

## A. Basic Subscriber Information

The CBA has consistently called for judicial authorization for the seizure of subscriber information. The former Bill C-30 proposed an administrative regime under which 'designated' peace officers could obtain subscriber information without judicial authorization. While the CBA supported some proposals in the Bill, in the area of basic subscriber information (BSI) we noted that the scope of the information listed was too broad, extending beyond what might be appropriately regarded as 'basic information'. There was no limit on how many customers' information could be demanded at once, and could be used to demand the names and addresses of all customers with IP addresses in a particular range. Finally, there was no mechanism for a telecommunications service provider to challenge an overly broad request.[15]

The Supreme Court of Canada has held that any demand for BSI must be authorized by a judge, be made in exigent circumstances or be based on a reasonable law. *R. v. Spencer*[16] requires an effective legislative response to govern the lawful seizure of subscriber information.

The Green Paper Backgrounder suggests that judicial authorization may be too onerous for the early stages of investigation, and that peace officers are unable to obtain information on a standard of 'suspicion.'[17] In fact, existing *Criminal Code* sections provide for judicial authorizations in the early stages of investigations on a threshold of 'reasonable suspicion.'

The most obvious template for judicially-authorized seizure of subscriber information is section 487.018, for seizure of bank account information. That section has the misleading title "Production Order – Financial Data," although it does not concern the substance of financial transactions. Instead, it concerns 'tombstone' data on financial accounts: account number, name, addresses, dates of opening and closing, and more. The information can be obtained by judicial authorization on a threshold of reasonable suspicion, appropriate to the earlier stages of investigation. If the production order process is unduly laborious and time-consuming, efforts could be focused on increasing the number of judicial officers available to review application, rather than removing important checks and balances.

When obtaining judicial authorization is impractical in situations of imminent harm or exigent circumstances, the obvious templates are sections 184.1 and 184.4 of the *Criminal Code,* which

---

15 This was seen as essential in *R. v Rogers Communications*, 2016 ONSC 70. That court suggested that a telecommunications service provider may have an obligation to assert the privacy interests of its clients.

16 [2014] 2 SCR 212.

17 Backgrounder at 57-58.

permit peace officers to intercept communications without judicial authorization in those circumstances. Section 184.4 was scrutinized by the Supreme Court of Canada in *R. v. Tse*, resulting in more stringent limitations.[18] In 2012, Bill C-30 included a provision for peace officers to obtain subscriber information without judicial authorization in defined exceptional circumstances and we suggest further consideration of such a provision.

Making judicial authorization the norm, with an administrative provision[19] for exceptional circumstances, would be preferable to a wholesale administrative regime of the type that has engendered inconsistency and controversy in other countries. Concerns about the scope and nature of the information, and the mechanisms by which it would be acquired must be measured against Canada's constitutional concept of a reasonable expectation of privacy. It is sometimes difficult to determine precisely where that threshold will fall but the Supreme Court has noted that this is a contextual exercise, requiring a careful balance between the rights of the individual and the legitimate interests of society in effective law enforcement.

As technology and investigative practices evolve, activities previously constitutional without a warrant may require a warrant. For example, the extent to which changes in technology and practice now allow for the discovery of core biographical information or reveal intimate details about lifestyle may mean prior judicial authorization is required. Further, the current technological capability to combine various sources of information to reveal additional details about individuals is significant, and may favour prior judicial authorization.

Administratively authorized search procedures, as opposed to court ordered procedures, have been shown to be particularly susceptible to abuse. In the United States, a recent review of National Security Letters issued under the *Patriot Act* revealed significant irregularities and abuse in the program. The Office of the Inspector General documented that the use of those letters increased exponentially after that power was expanded in the *Patriot Act*.[20] Difficulties and discrepancies in internal record keeping practices and controls complicated the task of compiling accurate information and statistics about their use. This experience should serve as a warning for Canada about administrative programs, as it shows that significant problems can arise even with a program that includes internal restrictions and safeguards.

---

18 [2012] 1 SCR 531.

19 See, *ibid*.

20 https://epic.org/privacy/nsl/

Our concern about warrantless access to BSI is heightened when the privacy interests engaged are unrecognized by those seeking change in this area, despite the *Spencer* decision. This might indicate an administrative process put in place outside of the oversight of an independent judicial officer would not be used sparingly.

## B. Interception Capability for Communications Services

The CBA urges caution in considering mandatory interception capabilities for communications services. Mandating interception capabilities, particularly without the involvement of the telecommunications service provider, can build backdoors that may be vulnerable to misuse. Encryption and interception capability would also have industry ramifications beyond the expertise of the CBA.

Any policy decision should also consider the many applications and other means available for sophisticated users to secure communications. The bottom line is that those wishing to evade interception (or encryption and data retention, below) have options, while ordinary Canadians could potentially become more vulnerable as the communications systems they use become less secure. In addition, we expect significant costs would be associated with building interception capabilities, which are likely to be passed on to consumers. Public consultation in this area should include that reality.

## C. Encryption

The Green Paper Backgrounder observes that any law intended to address encryption must consider:

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination;
- the investigative needs of law enforcement and national security agencies;
- commercial interests, such as competitiveness and the protection of intellectual property;
- how compelling decryption could weaken existing IT infrastructure models and systems;
- cybersecurity; and
- e-commerce.

Encryption safeguards online banking and the security of computers, and Canada's Privacy Commissioners have consistently recognized it as necessary to protect personal information when in transit. Encryption and virtual private networks also ensure that lawyers can work remotely while being confident that vital confidential client information is safe.

Proposals for law enforcement to obtain court orders requiring suspects to decrypt encrypted data or to provide their passwords raise significant issues, notably about the *Charter* right against self-incrimination. Practically, we question how such a law would operate. For example, if a key piece of information in a murder investigation was on an encrypted phone and the police obtained an order to compel disclosure of the password to that phone, a subject would presumably be compelled to cooperate. But, the punishment for not unlocking the phone would certainly be less than the punishment for murder, so the subject might be inclined to accept the consequences of refusing to abide by the order.

## D. Data Retention

Businesses in Canada are currently required to retain personal information for as long as necessary for the purposes for which it was collected. This is the law and it is common sense.

Businesses are also responsible for safeguarding personal information that they retain, and are liable if that information is compromised. Longer periods of mandatory retention would place businesses at greater risk of hackers and increase their costs. As discussed above, these costs are likely to be passed along to taxpayers at some point, and this reality should be made clear. As observed in the Backgrounder, the European Data Retention Directive has been found contrary to Europeans' privacy rights.

Police can already can make preservation demands on a threshold of reasonable suspicion (section 487.12) and judges can already make preservation orders on a threshold of reasonable suspicion (section 487.013). These provisions address the issue of data retention in the early stages of investigations, and we recommend that they should be tested in practice before further measures are considered.

**RECOMMENDATION**

**21. The CBA recommends that judicial authorization remain the norm for release of BSI to law enforcement, with an administrative provision for exceptional circumstances.**

**22. The CBA recommends that *Criminal Code* sections 487.12 and 487.13 be used to address data retention before further measures are considered.**

## XI. INTELLIGENCE AND EVIDENCE

The presence of intelligence in terrorism related proceedings, whether criminal, civil or administrative, is a problem that courts have grappled with more frequently in recent years. In some cases, the issue is disclosure of that information and, in others, it is about the actual use of information in proceedings. Ultimately, the federal government must balance the protection of national security information with *Charter* protected rights of individuals.

Currently, this balancing falls to designated judges on the Federal Court, either in the context of security certificate hearings or when section 38 of the *Canada Evidence Act* is triggered. A security-cleared lawyer (a special advocate) is mandated to protect the interests of the individual in security certificate hearings under the *Immigration and Refugee Protection Act*. Although not mandated, the Federal Court has been appointing security-cleared lawyers where disclosure of national security information is sought in criminal trials. Further, the Supreme Court of Canada in *R. v. Ahmad*[21] recently suggested that the use of special advocates may also be warranted in situations where a trial judge presiding at a criminal trial is trying to determine the effect of a section 38 non-disclosure order on the individual's right to a fair trial.

The CBA recommends that a security-cleared lawyer (whether a special advocate or *amicus curiae*) be used in all situations pertaining to national security where intelligence is either used in a proceeding or withheld from an individual where *Charter* protected rights are potentially compromised. Our adversarial system of justice requires both opposing parties to be able to put forward their respective positions and to have an impartial arbiter decide the issue. Using security-cleared lawyers in proceedings where national security information is at issue would help to ensure, although imperfectly, that the *Charter* rights of the individual are protected.

**RECOMMENDATION**

**23. The CBA recommends that a security-cleared lawyer be retained in all situations pertaining to national security when intelligence is either being used in a proceeding or withheld from an individual and the individual's *Charter* protected rights may be potentially compromised.**

---

21 2011 SCC 6.

## XII. CONCLUSION

The CBA appreciates the opportunity to again offer our views for consideration during the federal government's review of national security activities in Canada. We trust that they will be helpful, and would be pleased to offer further elaboration on any of the points raised in our submission.