CANADIAN MUSLIM LAWYERS ASSOCIATION

SUBMISSION ON BILL C-51, THE *ANTI-TERRORISM ACT, 2015*

House of Commons Committee on Public Safety and National Security

March 2015

CONTENTS

ABOUT THE CMLA

The Canadian Muslims Lawyers Association (CMLA) was founded in 1998 by a group of Toronto-based Canadian Muslim lawyers. It has over 300 members across Canada with active chapters in Ontario and Quebec.

The CMLA is focused on four key areas of engagement. First, the CMLA helps build professional relationships among Canadian Muslim lawyers and between Canadian Muslim lawyers and members of other legal organizations. Second, the CMLA educates its members and the broader Canadian Muslim community on law topics of interest. Third, the CMLA provides peer support by providing law students and junior lawyers with mentorship and professional development seminars. Fourth, the CMLA serves as an advocate on select issues of importance to Canadian Muslim lawyers and the broader Canadian Muslim community.

With respect to advocacy, the CMLA has appeared as a public interest intervenor before the Supreme Court of Canada. In addition, the CMLA actively participates in the discourse on national security law and policy. In this regard, the CMLA has made submissions to, and testified before, Parliamentary committees examining national security, human rights and civil liberties on numerous occasions since 2001.

SUBMISSION ON BILL C-51, THE *ANTI-TERRORISM ACT, 2015*

CANADIAN MUSLIM LAWYERS ASSOCIATION

OVERVIEW

The Canadian Muslim Lawyers Association (CMLA) is active in the discourse on national security law and policy in Canada. We have made submissions to, and testified before, Parliamentary committees examining national security, human rights and civil liberties on numerous occasions since 2001.

We are pleased to make a contribution to the study of Bill C-51, the *Anti-terrorism Act, 2015*, and national security law and policy more generally, because they are important matters for all Canadians.

A Faustian Bargain: Trading rights for a false sense of security

Bill C-51 should not become law because it grants the Government of Canada extraordinary, vague and unnecessary powers that threaten civil rights and privacy rights. In essence, Bill C-51 is a Faustian bargain: we trade our rights to gain a false sense of security.

Where new laws are demonstrably necessary to address national security challenges, such as terrorism, the CMLA supports measures that are consistent with the *Canadian Charter of Rights and Freedoms* (*Charter*) and the rule of law.

Bill C-51 is deeply flawed

While these submissions are not exhaustive, the CMLA's salient concerns on Bill C-51 are as follows:

- Bill C-51 reinforces the veil of secrecy and lack of accountability that Canada's national security agencies operate under.

- Although promoted as an anti-terrorism law, Bill C-51's reach extends far beyond terrorism.

- The broad definition of "activity that undermines the security of Canada" for information sharing purposes may pull non-violent dissent and activism into the national security dragnet.

- Unprecedented and wide-ranging information sharing based on vague and open-ended grounds puts the privacy and *Charter* rights of Canadians at risk. Furthermore, information may be shared beyond the express authority outlined in Bill C-51, including with foreign governments, their security agencies and the private sector.

- The no-fly list is created and administered in executive-controlled secret processes. Disclosing no-fly list information to foreign entities puts Canadians at risk. The process to remedy mistakes on the no-fly list is Kafkaesque.

- Data collected on all Canadians travelling by air may be kept indefinitely and disclosed broadly without a sound rationale that is linked to the purposes of Bill C-51.

- Expression far removed from criminal activity may be criminalized based on Bill C-51's vague language. The *Charter* right to freedom of expression may be chilled through self-censorship.

- Arrest without charge may be used as a form of *de facto* long-term control order, resulting in liberty restrictions without the benefit of a fair trial.

- Expanded powers for the Canadian Security Intelligence Service (CSIS) are antithetical to the McDonald Commission's recommendations, which led to the creation of CSIS as an intelligence-gathering agency separate from the Royal Canadian Mounted Police's (RCMP) work of policing.

- CSIS's new powers are overly broad and raise deeply troubling questions about the scope of illegal actions that may be taken to "reduce" threats to Canada's security.

- The use of judicial warrants giving CSIS extraordinary and unprecedented new powers to act illegally is contrary to the normal use of warrants. Moreover, asking judges to authorize *Charter* violations and illegal activity is inimical to the role of judges in our system of law and governance.

- CSIS's new powers are granted in secret processes and have no continuing oversight or supervision.

- The proposed amendments to the *Immigration and Refugee Protection Act* ignore the Supreme Court of Canada's ruling that secret evidence and proceedings are inherently unfair and unconstitutional.

These concerns and others are examined in more detail in the analysis section of this submission. Each part of the analysis below concludes by raising some important questions that are not answered in Bill C-51.

ANALYSIS

The CMLA takes the position that Bill C-51, the *Anti-terrorism Act, 2015*, grants the Government of Canada extraordinary, vague and unnecessary powers that pose a risk to civil rights and privacy rights. These powers fail to meet the objective of protecting our country from the threat of terrorism. In fact, Bill C-51 may result in wasting scarce resources by distracting us from genuine threats. This may ultimately harm Canada's public safety interests and erode public confidence in our national security system.

The Government has failed to demonstrate why new legislation that radically reshapes Canada's national security sector is necessary to address the challenges posed by terrorism. As many commentators have recognized, the problem of terrorism is not solved by reactive legal responses that infringe rights, but through positive community engagement, better intelligence, and effective enforcement.

Furthermore, the proposed powers are contrary to the recommendations of the Arar Inquiry,[1] as echoed in the Privacy Commissioner's 2014 report,[2] especially with respect to information sharing, independent review, oversight and accountability.

Where new laws are demonstrably necessary to address national security challenges, such as terrorism, the CMLA supports measures that are consistent with the *Charter* and the rule of law.

I. Scope Creep: Tenuous Connection Between Purpose and Powers

Bill C-51 is styled the *Anti-terrorism Act*. As such, it is reasonable and logical to assume that the proposed legislation is designed to address challenges posed by terrorism. Indeed, the Government of Canada's rationale and marketing on Bill C-51 makes that claim very clear.

> The world is a dangerous place and Canada is not immune to the *threat of terrorism*. *Terrorist attacks on our own soil* demonstrate that our law enforcement and national security agencies require more tools to keep pace with evolving threats, and to better protect Canadians here at home.
>
> In line with measures taken by our allies, our Government is taking additional action to help our law enforcement and national security agencies stop those who *promote terrorism*, including attacks on Canadians. We are also taking action to *prevent*

[1] *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar.*

[2] Office of the Privacy Commissioner of Canada, *Check and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance* (January 28, 2014), online: https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.pdf

terrorist travel and thwart efforts to use Canada as a recruiting ground, and prevent planned attacks on our soil.[3] (emphasis added)

This message is frequently repeated in background information provided by the Government on Bill C-51. Despite the purported purpose of responding to the threat of terrorism, the proposed legislation goes much further, giving broad and unprecedented new powers to security agencies and other federal departments. In reality, Bill C-51 is omnibus legislation laying the groundwork for a burgeoning National Security State.

For example, a vast information sharing scheme is created not only to address terrorism,[4] but also an unbounded and vague range of activities that "[undermine] the security of Canada", including interfering with the "economic or financial stability of Canada" or "critical infrastructure".[5] Scope creep and disconnection from the stated purpose of Bill C-51 is also apparent in the new CSIS powers to reduce, through active disruption, "[threats] to the security of Canada".[6] Clearly, the proposed CSIS disruption powers do not apply to terrorism alone, but the entire CSIS mandate, which is quite expansive.[7] This disconnection between legislative objectives and powers granted raises critical questions about the proposed legislation's consistency with the *Charter*. Arguably, Bill C-51 is constitutionally vulnerable because it lacks a rational connection between purpose and powers granted.

II. *Security of Canada Information Sharing Act* (SCISA)

A. Broad Information Sharing and Secrecy

Effective intelligence work in a free and democratic society requires focused information gathering, informed analysis and co-operation with others in a manner that is consistent with the rule of law and the constitutional values. SCISA fails to meet these standards.

SCISA introduces significant and unprecedented sharing of information between government institutions themselves and with foreign entities. Ultimately, privacy is threatened because information may be shared widely without appropriate supervision, protection and accountability.[8] This is particularly concerning in light of what two official Inquiries[9] tell us

---

[3] "Anti-terrorism Act, 2015", online: http://www.canada.ca/en/campaign/antiterrorism/

[4] In fact, the reference to "terrorism" as one of the activities that undermines the security of Canada is vague and problematic in itself. The term "terrorism" is not defined in SCISA and it is not clear how this term relates to "terrorism offences" and "terrorist activity" as defined in the *Criminal Code*.

[5] Section 2 of the *Security of Canada Information Sharing Act*, which is proposed as Part 1 of Bill C-51.

[6] Sections 12.1 and 12.2 of the *Canadian Security Intelligence Service Act*, which are proposed in clause 42 of Bill C-51.

[7] See section 12 of the *Canadian Security Intelligence Service Act*.

[8] The Privacy Commissioner of Canada has raised a number of concerns in this regard. Office of the Privacy Commissioner of Canada, *Bill C-51, The Anti-terrorism Act, 2015: Submission to the Standing Committee on Public Safety and National Security of the House of Commons* (March 5, 2015), online: https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp

[9] See Arar Inquiry and the *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nurredin*.

happened to Maher Arar, Abdullah Almalki, Muayyed Nureddin and Ahmad El Maati as a result of improper information sharing by Canada's security agencies.

The concerns about information sharing are compounded by Edward Snowden's revelations on the scope of information gathering, sharing, and Big Data analytics[10] taking place in the name of national security by Canada and its allies. We now know that vast amounts of personal information on millions of people, including Canadians, are being collected, analyzed, shared and stored in secret. One of the concerns about Big Data is that seemingly discreet and small pieces of information about an individual, when combined and analyzed with other information, can disclose significant profiles about that individual's life. Much like single pixels in a digital photograph, when taken alone they may seem irrelevant, but when combined with other pixels, they reveal a coherent image. SCISA establishes a foundation for whole of government information collection and sharing without appropriate rules and oversight; that is a recipe for serious trouble in a Big Data world. Figure 1 at the end of this section on SCISA attempts to provide a visual depiction of the whole of government approach to information sharing proposed by Bill C-51.

SCISA's failure to meaningfully address oversight, accountability, and include measures to ensure reliability and relevance of information, represent what Professors Kent Roach and Craig Forcese aptly describe as "Arar amnesia".[11] In many ways, SCISA is "anti-Arar", because it empowers staff in a wide range of government institutions (some having little or no national security expertise) to do things that the Arar Inquiry determined as one of the root causes of the problem: information sharing without appropriate safeguards and oversight. By refusing to learn from the tragic mistakes of the past we are doomed to repeat them.

A pervasive culture of secrecy throughout the information sharing scheme, and Canada's national security regime more generally, exacerbates the problems associated with massive and distributed information sharing.[12] Because almost everything happens in secret and with a multiplicity of decision points it will be practically impossible for adversely affected persons to find out why bad things are happening to them. Abuses of power, and even simple mistakes, will likely never see the light of day.

---

[10] Big Data analytics involves the collection and analysis of large amounts of information to determine patterns and predict behaviour. Intelligence agencies will argue that this can help identify risks for further scrutiny and interdiction. However, aside from a massive harvesting of information without reasonable cause, predictive analytics can yield false positives in terms of risk identification, which can have serious consequences on those flagged as risks. In addition, collection of massive amounts of information may also be counterproductive because security agencies will be lost in a forest of data and fail to see the one tree that requires attention.

[11] K. Roach and C. Forcese, "Bill C-51 Backgrounder #3: Sharing Information and Lost Lessons from the Maher Arar Experience" (February 16, 2015) online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2565886

[12] The proposed information sharing regime creates numerous decision points across government. This dispersion of control means there is no central decision-maker to maintain consistency of approach, ensure reliability of information being shared, and identify problems that may be emerging so corrective action can be taken. It is likely that the potential for mistakes and abuses under the proposed regime will increase on a scale reflecting the scope of information sharing that will take place.

Even if you do find that the source of your problems is government information sharing, SCISA immunizes the government from litigation, including where that behaviour is reckless or negligent.[13] Therefore, the claim that courts and judges are a shield against misuse of the powers in Bill C-51 is at best incorrect, and at worst disingenuous. Moreover, after the fact judicial vindications and compensation are an anemic substitute for a mature national security system imbued with robust accountability and a mindset of continuous improvement and respect for the rule of law.

B. Vague and Open-Ended Scope

SCISA's definition of "activity that undermines the security of Canada" is vague and overly broad.[14] The use of non-limiting language (*i.e.*, "including") to describe activities falling within the foundational information sharing definition leaves the door open for other activities to be added to the list. The vague and open-ended nature of this definition suggests that it may not survive *Charter* scrutiny. If the list of proscribed activities is to grow, SCISA does not provide any guidance on the process, criteria and accountabilities that will be used to expand the list.

Furthermore, non-violent dissent and activism may be characterized as undermining the security of Canada by the overly broad definition. Such a characterization will draw peaceful persons and organizations into the national security information collection, sharing, investigation and disruption dragnet. Once flagged as national security threats for "undermining the security of Canada" non-violent persons and organizations risk suffering a host of adverse consequences. For example, environmental, social justice and aboriginal activists may be guilty of undermining the security of Canada if they engage in activity that interferes with infrastructure, industries or products using "unlawful" non-violent means (*e.g.*, civil disobedience, marching without a permit, blocking roads, illegal pickets, illegal work stoppage/strike). SCISA's exemption for "lawful" advocacy, protest, dissent or artistic expression provides no protection in these cases. Contrast this approach with the *Criminal Code*, which does not include a "lawfulness" qualification for its exemption of advocacy, protest, dissent or work stoppage when defining "terrorist activity".[15] Unfortunately, the government has provided no justification for this inconsistency with existing law.

C. No Independent Supervision

SCISA lacks independent oversight and review. SCISA empowers staff across a wide range of government with broad discretion to determine when and how information will be shared within government.[16] Moreover, many of the institutions that SCISA grants new powers to are currently not subject to any independent review or oversight. As such, we are left with a "trust

---

[13] Section 9 of the proposed *Security of Canada Information Sharing Act*.

[14] See section 2 of the proposed *Security of Canada Information Sharing Act*, where "terrorism" is only one of a list of nine enumerated items that are considered to undermine the security of Canada. In addition, there is a striking lack of clarity with respect to "terrorism" as used in section 2 and how this term relates to "terrorism offences" and "terrorist activity" as defined in the *Criminal Code*.

[15] See section 83.01(1) *Criminal Code*.

[16] Section 5 of the proposed *Security of Canada Information Sharing Act*.

us" model of self-regulation, which creates ideal conditions for mistakes to be made, remain undetected, and grow into much larger problems.

It is unclear what the ultimate scope of each recipient institution's information sharing authority will be since the SCISA scope of authority is significantly broader than that found in each recipient institution's governing legislation. For example, SCISA's definition of acts that "undermine the security of Canada" is significantly broader than CSIS's authority under the *Canadian Security Intelligence Service Act* (*CSIS Act*).[17] In addition, consider that CSE's governing legislation restricts collection of information on and interception of communications of Canadians, while SCISA contains no such restriction.[18] Despite these significant mismatches in jurisdiction and authority, the proposed legislation provides no guidance or clarity on how these conflicts will be resolved. Arguably, SCISA could become a backdoor for scope creep with institutions acting far beyond their originally legislated mandates. For a sense of how these jurisdictional mismatches between individual institutions and SCISA interact with the broad information sharing authority see Figure 1 at the end of the SCISA section.

D. Unbounded Sharing Beyond Authority

Section 6 of SCISA is deeply problematic because it allows unbounded information sharing beyond the already vague and broad mandate outlined in section 2. The permissive language of section 6 indicates that once information is shared under SCISA a government institution receiving that information may then share it with "any person, for any purpose" so long as it is "in accordance with law". Figure 1 below provides a visual depiction of the potential scope of SCISA information sharing beyond the Canadian government.

This provision raises significant concerns about the use and sharing of information both within the Canadian government and with others, including foreign governments, foreign security agencies and the private sector. Of particular concern in this regard, SCISA does not have restrictions on sharing information with foreign governments and security agencies that have questionable human rights records.

Once information is shared beyond the Canadian government it is unclear how that information will be used and what further sharing may occur. As a practical matter, once information is released in this fashion it cannot be "reeled back" to correct errors or remedy mistakes. The consequences of these types of mistakes are not hypothetical. The tragic experiences of Maher Arar and others stand as stark reminders of why Canada needs appropriate rules and accountability in its national security system, especially with respect to information sharing.[19]

Additionally, section 6 of SCISA completely decouples the purpose for sharing information

---

[17] See "threats to the security of Canada" as defined and applied in sections 2 and 12 of the *Canadian Security Intelligence Service Act*.

[18] K. Roach and C. Forcese, "Bill C-51 Backgrounder #3: Sharing Information and Lost Lessons from the Maher Arar Experience" (February 16, 2015) at p. 32.

[19] Duffy, A. (February 24, 2015), "Almalki documents reveal Canadian authorities were unsure of evidence", *Ottawa Citizen*, retrieved from http://ottawacitizen.com/news/local-news/almalki-documents-reveal-canadian-authorities-were-unsure-of-evidence

both from Bill C-51's purported aim of responding to terrorism and SCISA's already broad scope of addressing activities that undermine the security of Canada.[20] In effect, this provision allows staff in recipient government institutions to share information for any purpose whatsoever once the initial sharing is triggered by the expansive "undermine the security of Canada" authority. This lack of a connection between the powers granted and the purpose of both SCISA and Bill C-51 suggests that section 6 of SCISA is very likely inconsistent with the *Charter* and principles of legislative coherence.

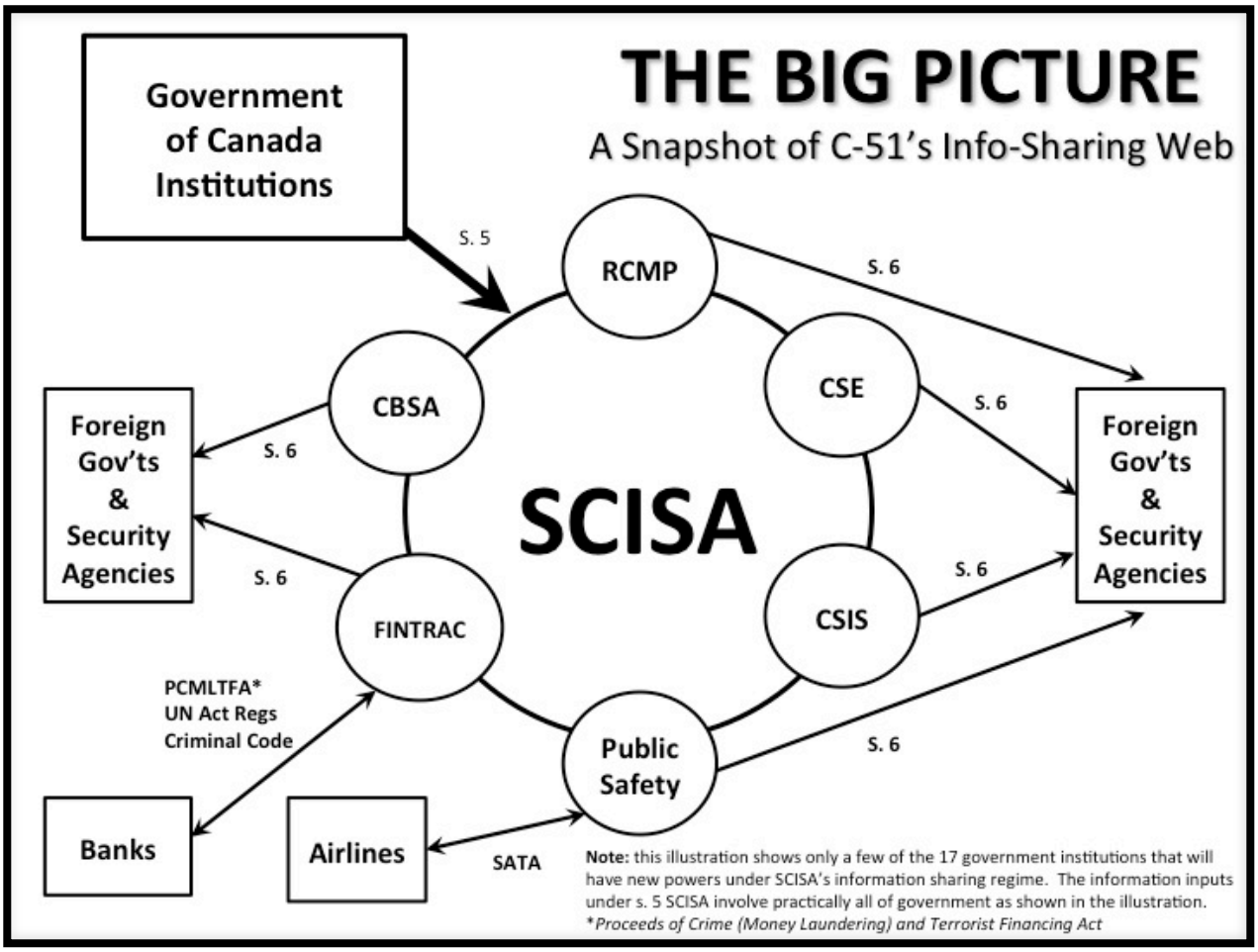

Figure 1: THE BIG PICTURE: A Snapshot of C-51's Info-Sharing Web

[20] Section 3 of the proposed *Security of Canada Information Sharing Act* states that "[t]he purpose of this Act is to encourage and facilitate the sharing of information among Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada."

E. Unanswered Questions

1. Who determines the unwritten content of SCISA's section 2 foundational definition?
2. What process will be used when adding activities to the enumerated list in section 2 SCISA?
3. Will the process to add activities to the section 2 SCISA list be open, transparent and accountable?
4. Will the expansion of the section 2 SCISA list be subject to independent review?
5. Will those who are subject to SCISA scrutiny have their information shared with foreign governments and security agencies, including those with questionable human rights records?
6. Will those who are subject to SCISA scrutiny be subject to other forms of national security investigation?
7. Why is the SCISA definition in section 2 broader than the definition of "threats to the security of Canada" in the *CSIS Act?*
8. How will CSIS operate when receiving or sharing information under SCISA in light of its own narrower authority under the *CSIS Act*?
9. How will CSE operate in light of conflicts between it's own mandate under the *National Defence Act* and SCISA's scope of authority?
10. How will conflicts between the mandate of the 17 recipient institutions in Schedule 3 and SCISA's scope of authority be resolved?
11. Will there be independent and transparent review, oversight and audit of the information sharing taking place under SCISA, as it extends to 17 different departments in Schedule 2 of the *Privacy Act*, many of which are subject to no independent review?
12. Why have the concerns that the Privacy Commissioner addressed in a January 2014 report about limits on powers to review information sharing, including international information sharing, not been addressed?
13. Will information obtained through torture be shared or used under the SCISA scheme?
14. How will reliability and relevance of information be ensured when shared under SCISA?
15. How will mistakes and erroneous information be corrected once shared under SCISA?
16. How long will shared information be retained by recipient institutions and will there be standards governing manipulation of data, derivative use and mandatory destruction?

III. *Secure Air Travel Act* (SATA)

SATA's stated purpose is ensuring "transportation security" and preventing people from travelling to commit terrorism offences abroad by using a no-fly list mechanism.

A. Secrecy and the No-fly List

The Minister of Public Safety and Emergency Preparedness creates the no-fly list, which is subject to Ministerial self-review every 90 days. The development and implementation of the list is undertaken in secret.

It is illegal for anyone to disclose that someone is on the no-fly list. As such, affected persons will find it extremely difficult to determine why they have been subjected to additional scrutiny or denied boarding as airline personnel are compelled by law not to disclose this information to

them. Although SATA includes a mechanism to challenge a listing, it is a Kafkaesque process fraught with flaws. The first hurdle for an affected person is actually finding out that s/he is on the no-fly list. If that hurdle is crossed and a challenge is initiated, affected persons are given no reasons for their listing or the determination of the Minister in response to the challenge; all of it is shrouded in secrecy.

Secrecy is not only wrong because it is fundamentally unfair, it is wrong because it generates untested, and therefore unreliable, information. Therefore, the efficacy of the no-fly list is questionable at best; it deems individuals to be security threats based on a secret process while denying them due process and the ability to defend themselves. In this form, no-fly lists create a false sense of security while having significant adverse impacts on the persons listed.

The no-fly list scheme in SATA is constitutionally suspect because similar secret processes have been found to be invalid by the Supreme Court of Canada in the immigration context.[21] Furthermore, the no-fly list scheme likely violates the *Charter's* guarantee of mobility rights.[22]

B. Sharing the No-fly List with Foreign Governments and Agencies

SATA indicates that the no-fly list may be shared with foreign entities.[23] Bill C-51 is silent on how this information will be used and controlled once shared beyond the Canadian government. It is plausible that information provided to foreign governments and their security agencies may be data-mined, compiled with other information in Big Data analytics and subject to derivative uses that have nothing to do with the express purpose of SATA. Once information is shared, especially with foreign governments and the private sector, it is impossible to retract in order to correct errors or remove from data banks. Therefore, once a mistake is made and data is shared it becomes a permanent and potentially viral mistake with cascading adverse consequences for the person to whom that data applies.

C. Building a Database of Air Travellers' Information

SATA allows the government to possibly maintain information provided by air carriers (*e.g.,* passenger information, itinerary, *etc.*) on those travelling by air for an indefinite time.[24] Arguably, in conjunction with SCISA this information could be combined with other data for data-mining and analytics in a Big Data context. This could contribute additional pieces to larger surveillance initiatives, allowing the government to do indirectly that which it cannot do directly.

---

[21] *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9. Processes similar to that found to be unconstitutional in *Charkaoui* are used in the listing of entities for terrorism purposes. Listed entities risk serious criminal sanctions and other adverse impacts in the private realm. Arguably, the use of secret evidence and proceedings in those contexts are inconsistent with the *Charter*.

[22] *Canadian Charter of Rights and Freedoms*, section 6.

[23] Section 12 of the *Secure Air Travel Act*, which is proposed as Part 2 of Bill C-51.

[24] Section 18 of the proposed *Secure Air Travel Act*.

D. Unanswered Questions

1. Why is there no independent scrutiny and oversight of the no-fly list, the process whereby it is created, and the manner in which it is implemented?
2. Will there be an independent audit and public reporting of the size of the no-fly list, as well as the list's errors, false positives and appeals on a regular basis to determine whether it is operating well?
3. Will information from foreign governments and security agencies, including those with questionable human rights records, be used in adding persons to the no-fly list?
4. Why is the Minister that creates the list in secret adjudicating appeals in secret from those listed?
5. Will an independent review body be established to hear appeals from those listed?
6. Will special advocates be involved to review and test secret evidence on behalf of the affected party during an appeal?
7. How will no-fly list information shared with foreign states and their security agencies be controlled to ensure that the information is not used for a purpose inconsistent with SATA, including sharing further with other governments and the private sector?
8. How will mistakes and errors be corrected in no-fly list information that is shared with foreign governments, their security agencies and the private sector?

IV. *Criminal Code*

A. Criminalizing Expression

The new offences of "advocating" or "promoting" terrorism offences "in general" are vague and far removed from actual criminal activity. This is problematic because it introduces criminal liability without a specific act and specific intent.[25] These offences are a departure from the fundamental rationale of our system of criminal law and the values embodied in the *Charter*.

In fact, existing terrorism offences already capture expression that is closer to criminal action.[26] The government has not explained why those provisions are inadequate and why this expansion of the criminalization of expression is necessary.

These offences may actually make it more difficult to investigate genuine terrorist threats by driving suspects underground. They will simply drop off the investigative radar by silencing their views on extremist violence. In addition, the proposed legislation may have further unhelpful consequences if police and security agencies focus efforts and resources on offensive expression that is far removed from criminality; resources will be wasted chasing "red herrings" while genuine threats may avoid detection and interdiction.

---

[25] See "in general" and "reckless" in proposed section 83.221(1) of the *Criminal Code*, which is introduced by clause 16 of Bill C-51.

[26] Instructing, counseling and threatening the commission of criminal offences, including terrorism offences, are already proscribed by the *Criminal Code*.

B. Putting the Chill on Expression

The proposed expression offences may chill legitimate expression involving topics such as foreign policy, national security and terrorism. The chilling may manifest in self-censorship, with people becoming wary of openly expressing dissenting, critical or unpopular views. This not only diminishes the public discourse, but also may harm genuine efforts to assist at-risk youth grappling with the lure of violent extremist ideas.

It is crucially important to distinguish offensive, unpatriotic and even vulgar expression from expression that directly incites criminal activity. The *Charter's* protection of expression as a fundamental right would be meaningless if it applied only to popular or anodyne views. Rather, fealty to freedom of expression in a mature democratic society is demonstrated when unpopular, disagreeable and even offensive ideas are aired without fear of legal sanction or bullying.

The provisions dealing with "terrorist propaganda" raise similar concerns to those outlined above because that term is also based on a vague definition of "promoting" or "advocating" terrorism offences "in general". Arguably, this provision may adversely impact expression and expressive material that legitimately examines or debates controversial issues (*e.g.,* self-determination movements, opposition to foreign dictatorships, national security policy). Moreover, discretionary application of the vague "terrorist propaganda" prohibition by government officials, such as border agents, may result in unjustified suppression of expression.[27]

C. Arrest Without Charge

The proposed legislation lowers the threshold for arrest without charge (recognizance with conditions), which is already an aberration in our system of criminal justice. This provision is problematic because it draws people into the criminal process and imposes restrictions on them without the benefit of clear charges, a fair trial and the right to full answer and defence. It may also lead to absurd outcomes where principled innocent persons are jailed for refusing to accept restrictions on their liberty as a condition of release, while dishonest criminals agree to conditions that they have no intention of respecting. A more effective approach involves focusing on investigations that build a sound evidentiary case as the foundation for criminal charges and trials. This would yield better results for both the accused and society; outcomes would be transparent and reliable, thereby strengthening public confidence in Canada's national security system while making Canada truly safer.

Lastly, if this provision is used in a revolving door fashion to effectively impose long-term conditions on suspects it may become a *de facto* control order. The result will be extended liberty restrictions without the benefit of evidence and a trial, which is not only unfair, but erodes confidence in our national security system.

[27] See *Little Sisters Book and Art Emporium v. Canada (Minister of Justice)*, 2000 SCC 69.

D. Unanswered Questions

1. If the provisions relating to prohibited expression are to become law, will free speech defences, as they currently exist in section 83.01(1.1) of the *Criminal Code*, be added to the proposed legislation?
2. Who will make decisions, and what criteria will be used, to determine the nature of "terrorist propaganda"?
3. What role will intelligence information play in arrest without charge and will it meet criminal law evidentiary standards?
4. Will evidence and intelligence information obtained from torture be prohibited from being used in arrest without charge?
5. Will special advocates be allowed to represent those arrested without charge in order to challenge secret evidence, intelligence information and government claims?
6. Would the lower thresholds for triggering arrest without charge in the proposed legislation have prevented the murder of Warrant Officer Patrice Vincent?
7. Will support of self-determination movements, groups opposing foreign dictatorships, and those critical of national security policy trigger the terrorist propaganda prohibition?

V. *Canadian Security Intelligence Service Act*

A. Ignoring the Lessons of the Past

The proposed legislation includes new CSIS powers to "reduce" threats to the security of Canada, which involve the ability to actively engage in a wide range of disruption activities.[28]

This radical expansion of powers is contrary to the public policy rationale and recommendations of the McDonald Commission that led to the creation of CSIS in the 1980s.[29] CSIS was established to separate intelligence gathering from police work because of illegal activities carried out by the RCMP Security Service while attempting to disrupt perceived threats, most notably from sovereignists in Québec. Therefore, the *CSIS Act* limits the scope of the agency's power to intelligence gathering; it cannot take police-like actions. The proposed amendments to the *CSIS Act* in Bill C-51 take us back to the pre-McDonald Commission era, bringing with them the very real risk that the mistakes of the past will be repeated.

The problems created by the blurring of lines between intelligence and police work was also examined in the Arar Inquiry; the RCMP's re-entry into national security work after 9/11 resulted in serious mistakes that contributed to Mr. Arar's plight in Syria.

B. Strengthening the Silos Between CSIS and the RCMP

Ironically, giving CSIS new police-like disruption powers may actually reduce co-operation between CSIS and the RCMP, making Canada less safe from the threat of terrorism. CSIS may

[28] Proposed sections 12.1 and 12.2 of the *Canadian Security Intelligence Service Act*.
[29] *Royal Commission of Inquiry into Certain Activities of the RCMP*.

develop an institutional mindset that views the RCMP's enforcement role as redundant in light of its own new powers to reduce threats through active disruption.

In addition, CSIS's new powers may present problems in terms of translating information gathered in the process of "reducing" threats into reliable evidence for viable criminal prosecutions of terrorism offences. The Air India Inquiry[30] warned of these dangers, but many of the recommendation for improving the transition from intelligence to evidence have not been implemented. The challenges with respect to intelligence and evidence also include the new CSIS source privilege in Bill C-44.[31] At the end of the day, all of this may jeopardize potential prosecutions and erode public confidence in Canada's national security system.

C. Enabling CSIS to Break the Law

Bill C-51 allows CSIS to obtain warrants authorizing its staff to contravene *Charter* rights or "be contrary to other Canadian law".[32] Given the findings of the McDonald Commission with respect to the illegal activities of the RCMP Security Service, it is strangely ironic that the government is proposing to give future illegal activities by CSIS the cover of legitimacy through law.

It is unclear how CSIS agents will interpret these authorizations to break the law. Will they seek broad authorizations of general actions and assume that all constituent actions under that general action are also authorized? For example, in an effort to infiltrate and disrupt a suspected plot threatening the security of Canada will they enable, participate in, or ignore criminal activity that furthers the larger plot, such as a bank robbery to obtain funds? This is particularly worrying given CSIS's track record of lack of candour with, and misleading of, courts and the agency's review body, the Security Intelligence Review Committee (SIRC).[33] CSIS also has a history of violating *Charter* rights. In one case an Ontario judge made the following observation when finding that CSIS agents acted unconstitutionally:

> The very people that are tasked by the federal government to oversee and safeguard Canada's national security are themselves acting in a manner that suggests either a complete lack of comprehension of our Charter rights or else, they demonstrate a total willingness to abrogate and violate these same principles.[34]

---

[30] *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182*.
[31] *Protection of Canada from Terrorist Act*, Bill C-44, 41st Parliament, 2nd Session, 2013-2014.
[32] See proposed section 12.1(3) of the *Canadian Security Intelligence Service Act*.
[33] See, for example, *X (Re)*, 2014 FCA 249 and *Almrei (Re)*, 2009 FC 1263. The Security Intelligence Review Committee (SIRC) has also flagged CSIS's lack of co-operation with respect to disclosure of information. More troubling, is SIRC's conclusion that is had been "seriously misled" and that the agency "violated its duty of candour" in secret proceedings before SIRC. Security Intelligence Review Committee, "Lifting the Shroud of Secrecy: Thirty Years of Security Intelligence Accountability" (Annual Report 2013-2014) at p. 3, online: http://www.sirc-csars.gc.ca/pdfs/ar_2013-2014-eng.pdf
[34] Justice Jane Kelly quoted in: B. Powell (October 6, 2010), "Toronto judge calls CSIS conduct 'reprehensible'", *Toronto Star*, retrieved from: http://www.thestar.com/news/crime/2010/10/06/toronto_judge_calls_csis_conduct_reprehensible.html In addition, the Supreme Court of Canada found CSIS to have seriously violated *Charter* rights with respect to Omar Khadr at the Guantanamo Bay prison; see *Canada (Prime Minister) v. Khadr*, 2010 SCC 3.

The scope of the warrant power also raises deeply troubling questions about civil rights violations and the potential for serious abuses. The warrant authorization language in the proposed amendments is open-ended and permissive, listing only a few extreme actions that are prohibited, including causing death or bodily harm, or violating the sexual integrity of an individual. One can only assume that anything that is not prohibited explicitly is allowed. Arguably, CSIS could engage in activities that result in psychological, emotional, social, economic and reputational harm, detention, rendition, harsh interrogation and the indirect causation of bodily harm by using foreign security agencies as proxies when the targets of their disruption activities are outside Canada.[35]

Judicial warrants should never authorize *Charter* violations and illegal activities. The use of judicial warrants to give CSIS extraordinary and unprecedented new powers is contrary to the normal use of the warrant mechanism in the criminal law. More importantly, judicial authorization to violate *Charter* rights and engage in illegal activity is antithetical to our system of law and governance; it turns our legal system on its head and conscripts judges as participants in the unsavoury business of dirty tricks.

Arguably, much of what will take place under the new warrants will never see the light of day as a result of secrecy and because CSIS will likely seek to "reduce" threats by direct interdiction rather than building a case for public criminal prosecution. Therefore, aside from the initial authorization of illegal activity in secret, courts will not play a continuing role in overseeing CSIS's disruption activities and remedying abuses. In fact, for many who will be targeted by CSIS's disruption activities, they may not realize the cause of the adversities visited upon them and their families, and as a result, will have no avenue for recourse or complaint.

D. Unanswered Questions

1. Will CSIS be able to detain people under the new warrant powers?
2. Will CSIS be able to interrogate people under the new warrant powers?
3. Will CSIS be able to inflict psychological, emotional, social, economic or reputational harm on targets under the new warrant powers?
4. Will CSIS be able to use rendition as part of a disruption strategy under the new warrant powers?
5. Will CSIS be able to indirectly engage in torture by using foreign proxies?
6. Will CSIS be able to disrupt the return of Canadian citizens to Canada in violation of their mobility rights under section 6 of the *Charter*?
7. Will special advocates be involved in the new warrant process to test CSIS's claims and make representations in the secret proceedings?
8. What independent review and oversight of CSIS's new powers will there be beyond initial judicial authorization of warrants?

[35] If these provisions will be accepted they should be improved by providing a tightly prescribed list of lawful actions that may be taken under the warrants rather than the current open-ended approach that authorizes illegal activity.

VI. *Immigration and Refugee Protection Act* (IRPA)

Bill C-51's proposed changes to Division 9 of the *Immigration and Refugee Protection Act* (IRPA) are contrary to fundamental *Charter* protections and the findings of the Supreme Court of Canada on the use of secret evidence in immigration and refugee proceedings.[36]

While Bill C-51 has been justified as a response to terrorism, the proposed IRPA amendments, as with many other elements of Bill C-51, reach far beyond the stated justification. Although the government suggests that the IRPA amendments only apply to a small set of cases (*i.e.*, security certificates), these new provisions will in fact apply to all IRPA proceedings where secret evidence is used. These proceedings include immigration detention reviews and appeals before the Immigration Appeal Division. The proposed changes will give the government additional powers to deny affected parties and special advocates adequate access to information to be informed of the case against them and answer it in a meaningful way.

Bill C-51 takes us back towards the uneven playing field of secret evidence that was struck down by the Supreme Court in 2007. The creation of the special advocate model was a response to the Supreme Court's finding that secret evidence and proceedings are inherently unfair and unconstitutional. Secret evidence is antithetical to our system of justice and the rule of law; its use is especially troubling where liberty and personal security interests are at stake.

Unfortunately, Bill C-51's proposed IRPA amendments set up the government as judge and jury in its own case, deciding what information is relevant and what should and should not be disclosed to special advocates. This is inconsistent with our legal system and the findings of the Supreme Court, and it is contrary to simple fairness and common sense.

VII. Building a Better National Security System

Bill C-51 is deeply flawed and unnecessary legislation that should not become law. Before integrating and concentrating more power in government agencies on national security matters, we should first implement the remedial findings of the many commissions of inquiry on the matter, most notably the Arar Inquiry.

Canada's national security agencies already operate under a veil of secrecy and lack sufficient accountability; Bill C-51 exacerbates this problem. This has at least three consequences: (i) resources will continue being wasted chasing "red herrings"; (ii) serious mistakes will go unaddressed and be may be repeated; and (iii) Canadians will not have an opportunity to assess and improve our national security work.

With national security functions becoming increasingly integrated it makes sense to have a concomitant and effective counterbalance in the form of an integrated independent oversight and review organization. Independent oversight and review should not be portrayed as "red tape" or

[36] *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9.

enemies of national security goals; rather, they can improve effectiveness and efficiency of national security work while building public confidence and trust.

The CMLA has consistently supported robust, independent and integrated oversight and review of Canada's national security sector and functions. While we do not endorse a particular form of oversight and review we believe it is important, at a minimum, that the following principles are reflected in that oversight and review body:

- Independent from national security sector and functions;
- Jurisdiction over all national security agencies and functions across government including CSIS, the CSE, the RCMP and a host of other agencies (some of which currently have no oversight and review);
- Full security clearance and access to national security information across government;
- Ability to initiate reviews and studies;
- Ability to initiate investigations and subpoena witnesses;
- Staffed by full-time civilian experts in national security law, policy and practice;
- In-house team of full-time special advocates to participate in secret proceedings involving national security across government;
- Budget funded by Parliament and secure from Executive tampering;
- Comprehensive public complaints and redress process including the ability to order remedies, including financial compensation;
- Ability to hear third party complaints;
- Participation and input from the public and civil society to build confidence and trust; and
- Annual audit and assessment of Canada's national security sector and functions to determine: (i) effectiveness and efficiency, (ii) impact on the rule of law and human rights, and (iii) how national security functions can be improved.

National security matters in Canada ought to be managed on a "lifecycle" model, which aims at continuous improvement. This could be achieved by feeding the knowledge gained through the annual audit and assessment back into the legislative and institutional design/reform process.

In conclusion, the CMLA is also keenly aware that Canadian Muslims have unfairly borne the brunt of Canada's national security law and policy since 2001. These ill effects have entered the private realm as well, with Canadian Muslims facing discrimination, stereotyping and xenophobia in everyday life. While the extraordinary powers of Bill C-51 put the rights of all Canadians at risk, experience tells us that Canadian Muslims will be disproportionately affected. A better way forward requires positive engagement, respect and co-operation with Canadian Muslims on matters of national security. This will not only build trust between communities, the government and security agencies, it will also result in more effective national security work that truly makes Canada safer.