Written Submission to the Standing Committee on Public Safety and National Security Regarding the National Security Framework

November 18, 2016

From the British Columbia Civil Liberties Association ("BCCLA")

Introduction

The BCCLA was pleased to appear before the Committee during both its hearings and its public consultation meeting in Vancouver. Our testimony to the Committee focused on the unnecessary and unprecedented surveillance powers granted under the *Security of Canada Information Sharing Act*, S.C. 2015, c. 20, s. 2, and the crisis of accountability with respect to surveillance conducted by Canadian intelligence agencies.

Our presentation to the Committee focused on recent findings by Security Intelligence Review Committee ("SIRC") as to the complete failure of Canadian Security Intelligence Service ("CSIS") to abide by the applicable legal standard in the collection of Canadians' personal information that populates the CSIS bulk data holdings. These extremely troubling findings by SIRC have since been compounded by the recent Federal Court decision that found that CSIS has breached its duty of candour to the court for a decade in relation to illegally collecting Canadians' metadata in violation of the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23 ("*CSIS Act*"). A further noteworthy development is that Quebec has recently launched an inquiry into the scandal of years-long surveillance of journalists that appears to have been partially facilitated by digital investigative powers that had been expanded by the *Protecting Canadians for Online Crime Act*, S.C. 2014, c. 31 (aka, the "*Cyber-bullying Act*").

We welcome this opportunity to supplement our testimony before the Committee with further written submissions. In this document we discuss:

British Columbia Civil Liberties Association
900 Helmcken Street, 2nd floor
Vancouver, BC, Canada V6Z 1B3
T 604.687.2919
F 604.687.3045
info@bccla.org
www.bccla.org

- **The need for repeal of the dangerous and unjustified powers granted by Bill C-51.**

- **The need to address the crisis of accountability in national security with a three-tiered accountability framework:**

    - amending Bill C-22 in order to create meaningful accountability through a Parliamentary Committee;

    - creating integrated expert review for all of the national security enterprises ("super-SIRC"); and

    - establishing the role of the independent monitor.

- **The need to repeal the Ministerial Directions allowing for the sharing of information derived from or likely to lead to torture.**

- **The need to bring appropriate judicial oversight to the activities of the Canadian Security Establishment ("CSE").**

- **Recommendations with respect to new digital investigative powers.**

- **The need to end the culture of impunity with respect to law-breaking by national security agencies and to squarely address the issue of the appropriateness and effectiveness of bulk-data surveillance and data analytics in the national security context.**

"Accountability" does not remedy dangerously flawed and over-broad laws

Our Association has had the privilege of participating in many aspects of the National Security Consultation. We appreciate how daunting a task it is to review Canada's national security framework and the magnitude of the work needed to have meaningful insight into the many complex technical and legal issues and the vast architecture of Canada's national security agencies and systems. We commend the government and the Standing Committee on Public Safety and National Security for undertaking this critically important task.

Given the complexity of the subject matter and the sheer volume of concerns that fall within the scope of this consultation, it is perhaps not surprising that there has been a propensity for government representatives to focus on accountability mechanisms, and in particular, place a very great emphasis on the role of the Parliamentary Committee that would be created by Bill C-22.

While we welcome the important discussion about the role of Parliamentarians in national security accountability, it must be bluntly stated that no committee, however constituted, can make amends for or provide meaningful accountability in the face of dangerous and recklessly overbroad powers granted to agencies working within national security.

It is imperative that the powers afforded to agencies involved in national security be measured, proportionate and demonstrably needed. The radical expansion of powers that were introduced by the *Anti-Terrorism Act, 2015*, S.C. 2015, c. 20, fail to meet this test.

We support the complete repeal of the measures enacted as part of Bill C-51, and that are now part of a range of different statutes. No aspect of that bill was ever demonstrably justified and the radical expansion of powers presents an even graver danger to the rights and security of Canadians in light of the now-anticipated reshaping of U.S. national security policy.

At the time of its introduction we made extensive submissions on Bill C-51 and we include a copy of those submissions for your review as **Appendix A**, along with our speaking notes from our recent presentation to your Committee as **Appendix B**. Rather than re-iterate points already covered, what follows will build upon them in the arenas that are either outside of "C-51" or that pertain to subsequent developments.

The failure of Bill C-22 to bring meaningful accountability to national security

We have certainly not heard of any individual citizen or representative of civil society who opposes the creation of a Parliamentary Committee to review national security agencies. However, there is a widely held view among those citizens and civil society members who have examined Bill C-22 that the proposal is insufficient and will fail to create public confidence.

Our Association's concerns about Bill C-22 track very closely the concerns we have seen contained in a detailed brief by the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic ("CIPPIC").

The most critical concerns are:

- The lack of independence of the Committee (which is apt to be, and be perceived as, a mere extension of the Executive);

- The inability of the Committee to ensure it receives relevant information;

- The inability of the Committee to initiate independent investigations; and

- The inability of the Committee to ensure substantially complete and robust reporting.

Canada has been singularly remiss in failure, until now, to introduce this national security accountability measure that many of our allies have long considered rudimentary. In undertaking this long-needed reform, now after many years of inaction, it is deeply concerning that Canada is proposing to replicate many of the acknowledged mistakes, since remedied, by jurisdictions that have had longer experience with such models.

Bill C-22, as it stands, represents a model of committee known to be flawed and inadequate. It is completely untenable to suggest a wait-and-see approach to a model that is already a cautionary tale and exemplar of what does not work.

Further, in addition to the myriad inadequacies of Bill C-22, there has been disappointingly little discussion and no concrete proposal to address the need for complementary integrated expert review of all the national security agencies, including those that currently operate with minimal or no oversight, like Canadian Border Services Agency ("CBSA") and Financial Transactions and Reports Analysis Centre ("FINTRAC"). Although the term may not represent the ideal model, the term "super-SIRC" is often used to discuss this. The need for a means of achieving a "super-SIRC" review cannot be overstated and is long overdue, having been vigorously recommended as long ago as the O'Connor Commission.

In addition to "super-SIRC" we also advocate for the UK and Australian model of independent monitoring. Canada has a great need for an independent monitor, with robust access to secret information, who is charged with providing an expert analysis of existing and proposed national security and national security-implicated legislation.

Why the three-tiered model of accountability is needed

There is no question that this three-tiered approach would create an accountability infrastructure that is more extensive than for other areas of government. However, this is necessary for two reasons.

1) *There currently exists a clear crisis of accountability in Canadian national security agencies.*

Canada has an unhappy reputation with respect to accountability in the national security realm. Canada was silent in response to the sweeping surveillance abuses disclosed by the Snowden revelations despite our indisputable involvement as a member of the Five Eyes and the obvious concerns for Canadians' rights. The on-going failure to implement the recommendations of three major inquiries on national security matters has further eroded public trust and confidence.

And, as previously alluded to, in only the past two months we have seen overwhelming evidence of a culture of impunity in relation to national security. Specifically, we have come to understand CSIS as essentially unmoored from lawfulness in an important range of its activities. It has been discovered to have breached its duty of candour to the Federal Court with respect to warrants of more than one kind, in some cases for more than a decade. And, on the basis of the recent Federal Court findings on bulk metadata warrants and the SIRC report's findings on its bulk data sets in total, it is now known that it is possible that the majority or even the entirety of bulk data in the CSIS holdings constitutes illegal spying on Canadians.

2) *National security accountability is unique.*

While all arenas of government require accountability, national security is unique in the seriousness of the consequences for both failures and abuses; the degree of operational secrecy required and the extent to which secrecy claims can be abused.

There is a growing recognition that one of the foremost challenges with respect to national security accountability is unearthing the numerous "secret laws" that are actually guiding the operation of our national security agencies. Canada's national security landscape is replete with secret laws that have no place in a democracy, where it is a fundamental aspect of the rule of law that laws be knowable and challengeable.

Secret laws come in many guises including secret legal opinions that provide de facto authority to interpret the provisions of statues in ways that range from unlikely to subverting.

The most recent SIRC report includes a timely example. This example pertains to interpreting the legal standard for collection of data in the *CSIS Act*. In SIRC's report we discover that CSIS takes the view that when it collects the personal information of Canadians that is open source and publically available, that that collection is not "collection" for the purposes of the statute and CSIS is, on that legal interpretation, allowed to take any and all of that personal information and use it in any fashion, without regard for the standard of "strict necessity" set out in the *CSIS Act*. Collection that is not "collection" is a very standard trope in national security agencies extending their surveillance powers beyond their statutory remit.

Secret laws also include secret ministerial direction and authorization and the secret body of law that grows from secret trials.

If we are to see confidence restored in accountability for our national security agencies, the members of the three-tiered accountability model (Parliamentary Committee, integrated expert review, independent monitor) must undertake a thorough audit of the many aspects of illegitimate secrecy that undermine the rule of law and separate those from arenas of legitimate operational secrecy.

Torture

Canada has a shameful history of complicity in torture. Canada's involvement in horrific practices includes active support for the Central Intelligence Agency ("CIA") torture program, including facilitating extraordinary renditions and helping to identify victims of such renditions, Maher Arar among them.

Currently, Canada is defying the recommendation of the O'Connor Commission with respect to policies governing circumstances in which Canada supplies information to foreign governments with questionable human rights records and the need for an absolute prohibition on providing information to a foreign country where there is a credible risk that it will cause or contribute to the use of torture.

Instead, despite the UN Committee against Torture calling for Canada to amend the dangerous practice, CSIS, the Royal Canadian Mounted Police ("RCMP"), the CBSA, CSE and the Canadian military all operate under Ministerial Directions which allow for collaboration and information sharing with foreign government agencies even if the information conveyed is derived from torture or torture may result.

At no time has this ever been acceptable. Torture is wrong and complicity in torture is wrong. Not only is it a violation of the most foundational of human rights, for which there is simply no justification, but it is dangerous from a national security perspective. As military and security experts have long pointed out, torture is not an effective means of acquiring intelligence. In fact it is almost guaranteed to provide faulty intelligence.

There is a great urgency for Canada to withdraw the existing Ministerial Directions on information sharing and torture. The chief prosecutor of the International Criminal Court has indicated her intention to investigate U.S. personnel for torture. Very significantly, the International Criminal Court's annual report outlined its findings on these alleged crimes, noting that they "were not the abuses of a few isolated individuals. Rather, they appear to have been committed as part of approved interrogation techniques in an attempt to extract 'actionable intelligence' from detainees". Further, as the President-Elect of the U.S. expressed vigorous support for torture in his campaigning, there is simply no justification for any attempt to dismiss concerns about information sharing and torture as remote or hypothetical.

Canada's current information sharing practices and protocols are in stark violation of the most basic human rights. It is imperative that Canada commit to a clear legal prohibition on sharing of information likely to be derived from or to lead to torture.

Appropriate Judicial Oversight of the Activities of the CSE

Our Association is currently in litigation with respect to the surveillance of Canadians by the CSE. We have heard, verbally, from the Minister of Public Safety that the government is committed to reforms in the oversight of the CSE. We urge the government to bring the activities of the CSE into compliance with Canadians' *Charter* rights.

Digital Investigative Powers

The government's Green Paper on the National Security Consultation includes a series of proposed expansions of police powers with respect to digital investigations. These powers do not pertain exclusively or even primarily to national security, but are rather general policing powers. We have commented on many of these extensively, but summarize some of our views here.

1) Basic Subscriber Data

What is currently termed Basic Subscriber Information ("BSI") is information about a telecommunications' customer and can include their name, address, phone number, email address, Internet Protocol ("IP") address and mobile device's unique identifier ("IMSI number").

As the Supreme Court of Canada set out in *R. v. Spencer*, 2014 SCC 43 ("*Spencer*"), there is a significant privacy interest in this information because it has the potential to expose a detailed biographical profile. The *Spencer* decision confirmed that this is not information that can be available to the police merely for the asking.

There are indications that the police would like to see an administrative-type warrant for this information, which would amount to a self-authorization regime, in which an officer is authorized by a designated officer to acquire BSI. We say that such an approach is insufficient.

Recommendation: BSI must be protected by court oversight on a standard appropriate to its significant privacy interest.

2) Data Retention

Preservations Orders are currently available from a judge on a very low standard to preserve digital information that police fear may be destroyed before warrants can be sought. The Green

Paper queries whether telecommunications companies should be required to retain customer data for long periods of time, just in case any of the data were to be sought by police in the future.

Extensive data retention is a security risk. Retaining personal data that is not necessary for a business purpose increases the risk of data breaches and violates a fundamental principle of data protection. In addition, blanket retention of the data of innocent people on a population-wide basis is very likely to be found a breach of the *Charter*. In 2014 the Court of Justice of the European Union struck down the EU "*Data Retention Directive*" as a breach of the *Charter of Fundamental Rights of the European Union*.

Recommendation: Evidence must be produced to show that current powers are insufficient before any consideration should be given to an approach that would weaken data protection for all Canadians and has already been rejected in Europe as a violation of fundamental rights.

3) Compelled Passwords/Decryption

Police have proposed that courts should be able to order individuals and businesses to provide passwords or facilitate decryption of materials that police have a warrant for acquiring.

This proposal is novel in Canadian law and such compulsion would clearly implicate the right against self- incrimination.

Recommendation: No proposal should be explored until we have court decisions on compelled passwords in the context of inspections by Canada Border Services Agency. There are cases that are already in progress and they will provide important guidance. If compelled passwords are not constitutional in the border setting (where the courts have ruled that there is a lower expectation of privacy), they certainly will not be constitutional in the setting of the ordinary criminal law.

4) Mass Surveillance Warrants

The Green Paper does not discuss a topic of great concern to many Canadians following revelations of Canadian police using mass surveillance devices called IMSI Catchers, more usually known as "Stingrays". These are devices which intercept cellphone data. It is clear that

the police are using these devices despite a number of police agencies maintaining a "neither confirm nor deny" stance with respect to their use.

Our current understanding is that police agencies are probably getting court authorization for use of the devices, although we have reason to believe that those authorizations are likely to be overbroad and leave the matter of what to do with the hundreds or thousands of people's data that are not the subject of the search entirely to the discretion of the police. We do not know if CSIS is using these devices, but we do know that CSIS refuses to even confirm to Parliament whether they take the position that they require a warrant if they were to use such devices.

In addition to mass surveillance devices, like Stingrays, the police also use mass surveillance techniques, like "tower dumps", which are production orders for phone records of massive numbers of people. We have seen a recent court case in which the warrants sought for "tower dumps" were found to be unconstitutional for sweeping over-breadth (affecting tens of thousands of people). The court also voiced concern that there were no statutory limitations to the police retaining the data of people who were never the suspects with respect to the warrants.

Recommendation: There should be a special warrant process for mass surveillance technologies and techniques. This warrant would ensure that law enforcement have these investigative tools available when necessary, while ensuring that individuals' rights are protected. This warrant process should also apply to intelligence agencies.

The culture of immunity and need for evidence-based policy and law

If there is, as evidence is increasingly showing, a culture of immunity in our national security agencies, it is likely in part caused by the habitual lack of repercussions for violations of the law in this sphere. To our knowledge, the government would be hard pressed to come up with examples of consequences brought to bear on national security personnel found to be violating the law. Indeed, evidence would suggest that a typical "consequence" of the discovery that national security agencies are breaking the law, is to quickly change the law to accommodate the violation, not punish the violator.

It should be entirely unsurprising that in the arena above all others that we are told we must invest trust and allow secrecy, that this pattern of encouraging impunity has been corrosive.

In our Association's view, the area that is gearing up to continue this pattern relates to the *CSIS Act* and its legal standard for data collection and use that has, on current evidence, been violated for at least a decade. The dangers of simply amending the *CSIS Act* to accommodate the illegal surveillance of Canadians are two-fold.

First, as just set out, the government would be complicit in endorsing law-breaking as a means to achieve law reform and further undermine public trust.

Second, so much of what we have discovered about unlawful surveillance in the national security realm pertains to bulk data, and is presumably of primary interest to the data collectors for the purposes of data analytics and profiling. The evidence on data analytics and profiling in the national security context is more extensive than is popularly known. It is extensive and almost definitive in its findings that these practices are often unsuited to deriving meaningful intelligence and that there is and can be no efficacious profiling for terrorism or serious crimes.

No meaningful democratic debate in Canada has, to our knowledge, ever been applied to the "big data" practices that are clearly fueling the wide-spread, mass surveillance of Canadians in the national security context.

We are very concerned that we are about to see a swift and sudden capitulation to long-standing defiance of the law with respect to unjustified surveillance and that this will exacerbate the already serious effects of racial and religious profiling in the national security realm.

We urge the government to resist the already-intimated calls (by CSIS) for reforms to facilitate population- based surveillance in the name of practices and policies that have never been justified or demonstrated to be effective in increasing public safety. An evidence-based approach to this matter would be called for at any time, but is particularly important as the government sets out to demonstrate its trustworthiness to the very communities most impacted by national security profiling in an attempt to bring about meaningful cooperation for programs to prevent radicalisation to violence.

Again, we thank the Committee for the opportunity to provide this supplemental submission on this very important subject of the national security framework for Canada.

All of which is respectfully submitted,

Micheal Vonn
Policy Director

APPENDIX A

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

SUBMISSION TO THE STANDING COMMITTEE ON NATIONAL SECURITY AND DEFENCE

Bill C-51, the *Anti-Terrorism Act, 2015*

April 2015 | Carmen K. M. Cheung, Senior Counsel

Executive Summary

In this brief, the British Columbia Civil Liberties Association sets out its chief concerns with Bill C-51, the *Anti-Terrorism Act, 2015*.

1. **The *Security of Canada Information Sharing Act* is fundamentally flawed and should not be enacted.** It endorses a radical conception of "security" unprecedented in Canadian law and an unbounded scope of what it means to "undermine" Canadian security. Based on these expansive concepts, the *Act* authorizes warrantless information sharing across government and dissemination outside of government. Such widespread and relatively unfettered access to personal information poses serious dangers to individual privacy; such extensive data collection and information sharing may also not necessarily benefit security. Moreover, the *Act* deepens an already serious deficit in national security accountability.

2. **The *Secure Air Travel Act* should be rejected.** As a threshold matter, we question the efficacy of no-fly schemes in general. Even if they do improve aviation security, the system proposed here suffers from serious procedural deficiencies. The proposed *Act* creates a system where travelers have no concrete way of knowing whether they are on the no-fly list, where the reasons for listings are largely kept secret, and where the judicial process for reviewing delisting applications can be held in secret. This is a dangerous lack of due process. Where warranted, travel bans should be imposed pursuant to a court order.

3. **We oppose the creation of an advocating or promoting terrorism offence in the *Criminal Code*.** While any chilling of speech has serious consequences for democratic life, expressive chill in this context also impacts security and public safety. To the extent that monitoring extremist speech can aid in investigating security threats and protecting public safety, the chilling effect of the proposed offence may drive that speech offline or underground. We see no security interest in further criminalizing expression beyond what is already proscribed by law.

4. Bill C-51 expands a troubling regime of preventative detention by lowering already low thresholds for detaining individuals on mere suspicion of dangerousness. Before asking what additional powers are required to protect public safety, we need to determine how well existing powers are being used and whether existing criminal law is being properly enforced. **The proposed amendments relating to recognizances with conditions should be rejected.**

5. By giving CSIS the power to engage in "threat disruption", Bill C-51 blurs the line between spying and policing carefully drawn following the McDonald Commission. We are deeply troubled by the proposed CSIS warrant powers in this Bill, and the proposition that Canada's courts should be tasked with authorizing measures that violate constitutional rights. This profoundly misconstrues the role of the court in our constitutional system. **The proposed amendments to the *CSIS Act* are unwise and unnecessary, and should be rejected.**

6. Bill C-51 ignores the Supreme Court of Canada's teachings that the government cannot rely on secret evidence in security certificate proceedings without providing some way for the named person to know the case to be met, and a procedure by which the evidence could be tested. **The proposed amendments to IRPA which would limit the scope of materials produced to special advocates should be rejected.**

Introduction

The British Columbia Civil Liberties Association ("BCCLA") is one of Canada's oldest and most active civil society organizations. Our mandate is to preserve, defend, maintain and extend civil liberties and human rights in Canada. We are an independent, non-partisan organization. We speak out on the principles which protect individual rights and freedoms, and have played an important and prominent role on almost every significant national security-related civil liberties issue for over 50 years.

Nowhere is the BCCLA's national presence and expertise more evident than in the roles it has played in the development of policy on national security, intelligence and anti-terrorism matters. The positions taken by the BCCLA are based on the guiding principle that in a democratic society, restrictions on basic rights and freedoms are justified only if they are ultimately necessary for the sake of protecting those very rights and freedoms.

The BCCLA's submissions on Bill C-51 focus on six main areas of concern:

1. The enactment of the *Security of Canada Information Sharing Act*;
2. The enactment of the *Secure Air Travel Act*;
3. The proposed advocating or promoting terrorism offence in the *Criminal Code*;
4. The proposed amendments to recognizances to keep the peace relating to suspected terrorist activities or terrorist offences (preventative detention);
5. The creation of new powers for the Canadian Security Intelligence Service ("CSIS") to "reduce" threats to the security of Canada; and
6. Increased restrictions on access to information by special advocates in security certificate proceedings under the *Immigration and Refugee Protection Act* ("IRPA").

Our comments address both the constitutionality of the proposed provisions, as well as their wisdom and necessity. We hope that as this Committee examines Bill

C-51, it will consider not only whether its proposed provisions are legal and constitutionally compliant, but whether they are also efficacious and just.

1. The enactment of the *Security of Canada Information Sharing Act*

The *Security of Canada Information Sharing Act* (the "*Information Sharing Act*") is fundamentally flawed and should not be enacted.

Radical conception of "security" and unbounded scope of what it means to "undermine" Canadian security

The basic premise of the *Information Sharing Act* is to "encourage and facilitate information sharing between Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada." As defined in the proposed *Act*, this means any activity that "undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada." This includes activities that relate to not just public safety, but to public life in general, including "the administration of justice" and "the economic or financial stability of Canada". It even extends to activities that "undermine the security of another state". Because "people of Canada" is defined in the proposed *Act* as including any citizen or permanent resident (with no limitation on where they might be located), the *Act* can apply to *any* activity that undermines the security of *any* Canadian, *anywhere in the world*. While "security" is very broadly defined, there is no definition or clarity provided for the very subjective concept of what it means to "undermine" security. Thus, we would agree with national security experts Kent Roach and Craig Forcese, who have observed that such an expansive understanding of "security" is "wildly overbroad" and "unprecedented" in Canadian law.[1]

The amended version of Bill C-51 presented before this Committee now explicitly excludes all "advocacy, protest, dissent and artistic expression" from the definition of "activity that undermines the security of Canada". While this amendment is welcome, we remain concerned that the broad definition of security will continue to capture expressive activities. Indeed, recent examples

[1] Kent Roach and Craig Forcese, Bill C-51 Background #3: Sharing Information and Lost Lessons from the Maher Arar Experience (February 16, 2015) (Backgrounder #3) at 7. Available at http://ssrn.com/abstract=2565886.

show that government already takes a very wide view as to what constitutes a threat to Canada's security. We know that CSIS and the RCMP – institutions responsible for ensuring public safety and national security – have monitored non-violent protests undertaken by First Nations and environmental groups opposed to the proposed Enbridge Northern Gateway Pipeline project. Last year, the federal Government Operations Centre called on all federal departments to compile information on every single protest happening in Canada, ostensibly to build and share "common situational awareness at the national level related to all hazards of national interest, emerging or occurring."

The radically expansive concept of security contained in the proposed *Act* has the potential to colour how government and law enforcement agencies determine what constitutes a threat to security, leading to unwarranted and unnecessary scrutiny into the private lives of many Canadians. As the experiences of Maher Arar, Ahmad El Maati, Muayyed Nureddin and Abdullah Almalki show, a sweeping conception of "threat to Canadian security" coupled with liberal information sharing practices can have devastating results.

"All of government" access to personal information and wide-ranging information sharing

Section 5 of the proposed *Act* authorizes warrantless information sharing between government institutions, either by request from one institution to another, or on the initiative of the institution originally possessing the information, if it believes that the information is relevant to the receiving institution's security-related responsibilities. Such responsibilities include "detection, identification, analysis, prevention, investigation or disruption" of "activities that undermine the security of Canada". Section 5 also explicitly contemplates ongoing dissemination of this information – thus, intelligence originating from CSIS can be shared with the Royal Canadian Mounted Police ("RCMP"), who might then pass it on to any of the other government institutions authorized to share information under this regime. Bill C-51 sets out 17 such institutions in its Schedule 3, which includes the Canada Revenue Agency and Health Canada – institutions which traditionally have had little responsibility (or jurisdiction) over matters relating to national security. All it takes to expand that schedule is regulation from the federal Cabinet; no Parliamentary input or consideration is required. The logic of the proposed *Act* appears to be that if all

individual conduct can be related to security, then everyone in government is responsible for security.

As wide-ranging as that may seem already, the proposed *Act* does not simply limit information sharing to the scheduled institutions. Section 6, as it was originally tabled in the House of Commons, read as follows:

> For greater certainty, nothing in this Act prevents a head, or their delegate, who receives information under subsection 5(1) from, in accordance with the law, using that information, or further disclosing it to any person, for any purpose.

The amended version of Bill C-51 before this Committee contains a revised Section 6, which reads as follows:

> For greater certainty, the use and further disclosure, other than under this Act, of information that is disclosed under subsection 5(1) is neither authorized nor prohibited by this Act, but must be done in accordance with the law, including any legal requirements, restrictions and prohibitions.

This amendment, however, is a distinction without a difference. While the formulation has changed, the essential substance of this clarification is the same – any receiving agency is free to further disseminate information to any person, for any purpose, so long as it is "in accordance with the law".

The concerns raised by Professors Roach and Forcese with respect to the original Section 6 have equal application here: existing law governing information sharing is thin, and to the extent it exists in legislation like the *Privacy Act*, is "riddled with exceptions and limitations" to its reach.[2] For example, s. 8 of the *Privacy Act* sets out 14 different exemptions to the general prohibition against disclosure of personal information without the consent of the individual to whom that information relates.

One such exemption allows personal information under the control of a government institution to be disclosed for "any purpose where, in the opinion of

[2] Backgrounder #3 at 14.

the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure." The public clearly has a strong interest in ensuring that Canada's security is protected, but when Canada's security is conceived of in terms as broad as those set out in this *Act*, the range of activities that could serve as justification for massive information sharing is dramatically expanded. And when the aim is to identify threats (as opposed to tracking known threats), there is nothing in this legislation and in the existing privacy legislation to prevent government institutions from either requesting or offering up entire databases for review by any of the scheduled institutions.

Moreover, examples like the Minister of Public Safety's directives to security agencies to engage in international information sharing even in situations where it might result in torture – which plainly violates international law – show that the question of whether existing practices are "in accordance with law" is far from settled.

It is obvious that such widespread and relatively unfettered access to individuals' information by all of government (and made available outside of government subject to government's interpretation of what is legal) poses serious dangers to personal privacy. What should also be clear is that such extensive data collection and information sharing may not be good for security or public safety, either.

What this proposed *Act* essentially does is designate a great many things as relevant to "security", and then directs government institutions to either solicit or proactively share any information that can conceivably be related to "security". The bureaucratic default would be to request and provide as much information as possible, given that few institution heads will want to be responsible for failing to disclose or request potentially relevant information should a security failure occur.

Massive information, however, does not necessarily translate into better security. An excess of information may make it even more difficult to identify real security threats – when looking for a needle in a haystack, simply adding more hay does little to help the effort. Requiring government institutions to make targeted and tailored requests for information is not only better in terms of protecting privacy – it helps ensure that crucial intelligence and information does not get lost in a sea of data.

No corresponding "all of government" review and oversight and continued erosion of accountability

There are two primary limitations on information sharing in the proposed *Act* – that the sharing must be done "in accordance with law", and that information must be "relevant to the recipient institution's jurisdiction or responsibilities". However, the nature of national security activities and the opaque information-sharing regime created by the proposed *Act* means that it is difficult to tell whether government is acting lawfully, and within the limitations imposed by the *Act*. There is no mechanism in the *Act* to alert an individual that her

information has been passed on from one government agency to another, let alone that her information has been shared outside the government. Even if she were to seek out that information directly, the fact that the information sharing is authorized for "security" reasons may cloak all relevant details in national security secrecy. Judicial intervention would likely be limited, and perhaps primarily only in response to complaints from individuals or civil society who are somehow alerted to misconduct. Accordingly, the only way the public can have confidence that information sharing is lawful and appropriate is through robust review and oversight.

Since 2001, we have seen increased inter-institutional cooperation across all sectors of government when it comes to addressing national security concerns. This proposed *Act* is only the latest of such efforts. However, inter-institutional accountability has not developed in parallel. There is, on the one hand, increased cooperation between government institutions in terms of sharing information and engaging in joint investigations and operations. On the other hand, review bodies such as the Security Intelligence Review Committee ("SIRC"), the CSE Commissioner, and the Complaints Commissioner for the RCMP are still siloed and segregated into their own narrow jurisdictional confines. No similar legislative efforts have been made to allow for an "all of government" review for "all of government" activities. This lopsided development of the national security apparatus has resulted in a serious accountability deficit.

Bill C-51 furthers this imbalance. Provisions in the *Information Sharing Act* erect even more barriers to accountability. Section 7 of the proposed *Act* attempts to limit the scope of disclosure obligations in court proceedings such that the information-sharing institution is not bound by the same disclosure requirements

as the information-receiving institution.

Suppose the RCMP is conducting an investigation, which leads to criminal charges being laid against an individual. As part of its investigation, the RCMP has received information from CSIS. Section 7 of the proposed *Act* does away with any presumption that CSIS and the RCMP are engaged in a joint investigation, and that both institutions must make the same types of disclosure to the accused. Thus, while the RCMP may be required to disclose both inculpatory and exculpatory evidence, CSIS may not be subject to these same obligations. This can create serious problems in terms of testing the reliability of the source information, and incentivizes selective sharing of information between institutions. Using the same example of CSIS and the RCMP, CSIS can simply withhold potentially exculpatory information from the RCMP. Neither the RCMP nor CSIS would be obliged to provide it to the accused, since it is not information in the RCMP's possession and CSIS is not automatically subject to the same disclosure obligations. Rather than the burden being on the government to make sufficient disclosure to the accused so that his fair trial rights are respected, it will be up to the accused to seek it.

Section 9 creates a qualified immunity against civil suits arising from "good faith" information sharing. At the clause-by-clause review of this Bill conducted by the House of Commons Standing Committee on Public Safety and National Security ("SECU") on March 31, 2015, counsel for Public Safety Canada stated that this provision simply creates a qualified immunity for individuals acting in "good faith", and that proceedings against the Crown for harms resulting from "good faith" information sharing remained available. Knowledgeable commentators, however, have interpreted this section as potentially foreclosing civil suits altogether, which suggests that the scope of the immunity requires clarification.

Civil liability for government conduct resulting in harm serves as an important form of accountability. Civil liability not only provides an important form of redress to individuals, but serves as a powerful deterrent to future misconduct and reminds government of its duties and obligations to all Canadians. Immunizing "good faith" information sharing (even in cases where information sharing may lead to torture or death) means that the burden is on the victim to demonstrate that government agents acted in bad faith – a very high bar. And in the case where the resulting harm from government action may take the form of a

Charter breach, a qualified immunity simply has no place: the government is never permitted to violate an individual's constitutional rights, whether in good faith or bad.

It is our submission that this Committee should reject the *Security of Canada Information Sharing Act* in its entirety.

2. The enactment of the *Secure Air Travel Act*

Since June 2007, Canada has utilized a "no-fly" scheme known as the Passenger Protect Program. Under the current scheme, the Minister of Public Safety creates a no-fly list based on the recommendation of an advisory group comprised of representatives from Public Safety Canada, Transport Canada, CSIS, the RCMP, the Canada Border Services Agency ("CBSA") and Justice Canada. Listing decisions are reviewed every 30 days. The list is provided to Transport Canada.

Transport Canada, in turn, provides the no-fly list to airlines. The list provided to airlines is also updated every 30 days. Airlines are required to screen all passengers against this list, and to contact Transport Canada if anyone on the list attempts to board an aircraft. At that point, Transport Canada determines whether that traveler "poses an immediate threat to aviation security". If so, the Minister of Transport issues what is known as an "emergency direction" and the traveler is not permitted to board. The traveler, however, is otherwise free to leave the airport and board other modes of public transport.

Under the current scheme, individuals know that they are on the Canadian no-fly list when they provided with the "emergency direction" when attempting to obtain a boarding pass. They can challenge their listing by making an application to the Office of Reconsideration. The Minister of Public Safety reviews these applications and determines whether an individual should remain on the no-fly list.

Canada's no-fly regime has never been comprehensively legislated, and exists primarily as a creature of regulation and guideline passed under the auspices of the *Aeronautics Act*. The *Secure Air Travel Act* purports to finally create a legislative framework for Canada's no-fly list. It is, however, deeply flawed.

As a threshold matter, we question the efficacy of no-fly schemes in general.

Travelers on such lists are deemed too dangerous to fly, yet too harmless to arrest. They are restricted from boarding aircraft, but not trains, or ferries, or subways, or buses. There is little evidence that no-fly schemes increase aviation safety and security.[3]

Even if no-fly lists do have an effect on aviation security, the system proposed under the *Secure Air Travel Act* raises serious procedural concerns.

As with the Passenger Protect Program, the Minister is empowered to establish a no-fly list. Under the proposed *Act*, an individual can be listed if the Minister has
Page 11/23 reasonable grounds to suspect that he or she will

(a) engage or attempt to engage in an act that would threaten transportation security; or

(b) travel by air for the purpose of committing certain terrorism offences as outlined in the *Criminal Code*.

Instead of reviewing the list every 30 days, the *Act* only requires the Minister to review it every 90 days to determine whether everyone listed continues to meet the criteria for listing. Under this new scheme, there are two consequences to listing. Listed persons may either be prohibited from flying, or they may be subject to additional screening at the airport. Unlike with the Passenger Protect Program, no written "emergency direction" is issued to the affected person. In fact, the proposed *Act* makes it illegal to disclose whether an individual is on the list or not, creating an absurd situation where neither government nor airlines can confirm or deny listings, even to the person affected.

The opacity is compounded by the fact that prohibition against flying is only one of two consequences of being listed. Travelers may simply be repeatedly subjected to additional screening at airports. Given that they cannot be informed of their listing, they will simply have to guess as to whether the additional

---

[3] If law enforcement officials have enough information to determine that an individual poses a threat to aviation safety, or that they are planning to board a plane in order to commit a terrorism offence, they are also likely to have enough information to lay charges or seek a recognizance order with conditions. The criminal law as it already exists also allows the government to impose travel bans pursuant to a court order.

screenings are simply an unlucky run of random secondary searches, or if they are the result of being on a no-fly list. If it is the latter, the proposed *Act* provides no mechanism for seeking a delisting. Under Section 15 of the *Act*, only individuals who have been denied transportation may seek to have their names removed from the list.

The delisting process is rife with procedural deficiencies.

When applying for a delisting, the individual knows only that she has been denied the ability to board an aircraft. She is not informed of the reasons for her listing. Her task is to prove a negative – that she is not a threat to aviation security and that she is not about to commit a terrorist offence. The Minister is given 90 days to make a decision on the delisting application. If no decision is rendered, then the individual is deemed to remain on the list.

At that point, the listed person can seek judicial review of the Minister's refusal to delist, though for individuals who have been "deemed" to remain listed, there is no actual decision to appeal from. In those cases, the appeal is undertaken with no record, and no information concerning the reasons for listing. Once the appeal is underway, the government presents the court with information relevant to the listing. The affected person has no access to this information. At best, the affected person is provided with a summary of reasons for listing, but the underlying evidence itself can be withheld on national security grounds. Under the proposed *Act*, the summary of reasons need not be complete; a judge may rely on information supplied by the government even if no summary of that information has been provided to the affected person. There is no requirement that exculpatory information be provided to the judge for consideration. Finally, if the Minister requests it, the hearing of the appeal *must* be held in secret – neither the affected person nor counsel is permitted to attend.

The *Secure Air Travel Act* creates a system where travelers have no concrete way of knowing whether they are on the no-fly list, where the reasons for listings are largely kept secret, and where the judicial process for reviewing delisting applications can be held in secret. This is a dangerous lack of due process. As a United States federal court recently held in a case striking down the redress regime for the US no-fly list, lack of information concerning the reasons for listing combined with the "low evidentiary threshold" for being placed on a list in the

first place creates a "high risk of erroneous deprivation" of constitutional rights.[4]

While individuals on the list are not permitted to access information relating to their own listing, the proposed *Act* does allow the government to share its no-fly list with other governments, with no statutory limitations on how that information can be used by the foreign state. Canada's experience with mistakenly labeling individuals as security threats and providing that information to foreign governments should counsel against such carte-blanche approaches to foreign information-sharing.

It is our submission that this Committee should reject the *Secure Air Travel Act* in its entirety. Where warranted, travel bans should be imposed pursuant to a court order, not as a result of discretionary executive decision-making.

The amendment adopted by SECU to Section 9 of the proposed *Act* does not assuage any of our concerns. It simply applies to the actions that airlines must undertake to give effect to the no-fly list, and does not address the question of whether no-fly regimes are effective in general, or the procedural infirmities specific to the no-fly scheme proposed here.

3. The proposed advocating or promoting terrorism offence in the *Criminal Code*

Bill C-51 seeks to amend the *Criminal Code* by creating the offence of advocating or promoting terrorism. The proposed offence would criminalize speech and sentiments – even those expressed privately – that "advocates or promotes the commission of terrorism offences in general". Unlike the hate propaganda offence that it is based on, the new advocating or promoting terrorism offence contains no exemptions for private conversations or statutory defences, such as a public interest defence. The proposed offence also introduces the troublingly open-ended language of "terrorism offences in general", which appears to go beyond the already broad definition of "terrorist activity" set out in s. 83.01 of the *Criminal Code*. As Professors Roach and Forcese have observed, "this is a

[4] *Latif v. Holder*, 969 F.Supp. 2d 1293 (D. Or. 2013).

potentially infinite number of offences."[5]

We see no security interest in further criminalizing expression beyond what is already proscribed by law. The *Criminal Code* makes it illegal to counsel anyone to commit a terrorism offence – considering that terrorism offences include acts that fall well short of violence, such as preparing to commit terrorist acts or supporting terrorist activity, this already captures a broad range of terrorism-related expression. The participating, facilitating, instructing and harbouring provisions in s. 83.18, *et seq.* contemplate recruitment and instruction (both directly and indirectly) to commit terrorist acts as criminal offences. In *R. v. Khawaja*, the Supreme Court of Canada considered the constitutionality of the definition of "terrorist activity" in the *Criminal Code*, and allowed it to include "threats of violence".[6]

At SECU's clause-by-clause review, the director of the Department of Justice's Criminal Law Policy Section suggested that the existing *Criminal Code* prohibitions on terrorism-related speech did not sufficiently capture all expressive modes that constituted "active encouragement" to commit a terrorism offence. But government has yet to provide a single example of the type of problematic speech that it hopes this provision would capture, which is not already caught by the existing *Criminal Code* offences. It has failed to give any concrete justification for the creation of such a sweeping offence.

The reach of this new offence goes well beyond "active encouragement" to engage in terrorism. What this offence would do is make criminals of individuals who have neither committed, nor plan to commit, any criminal or violent act. It would make criminals of individuals who are neither counseling nor inciting acts of terror or violence. It would make criminals of individuals whose sentiments may never even leave the confines of their own living room, so long as their speech can be seen as advocating or promoting terrorism "in general" to someone who might commit a terrorism offence. The new offence contains no requirement that the speaker actually intends for a terrorist offence to be committed. In fact, it contains no requirement that a terrorist offence be committed as a result of the

---

[5] Kent Roach and Craig Forcese, Bill C-51 Backgrounder #1: The New Advocating or Promoting Terrorism Offence (February 3, 2015) at 14. Available at http://ssrn.com/abstract=2560006.

[6] *R. v. Khawaja*, 2012 SCC 69 at para. 73.

impugned speech.

Government may say: we do not intend to prosecute teenagers for comments made on social media. But the ambit of the proposed offence is such that the type of speech that is ultimately criminalized will be a matter of prosecutorial discretion.[7] It is a foundational principle of criminal law that "prohibited conduct must be fixed and knowable in advance".[8] Even if prosecutions were limited, expression would be chilled.

Any chilling of speech has serious consequences for democratic life, but expressive chill in this context also impacts security and public safety. To the extent that monitoring extremist speech can aid in investigating security threats and protecting public safety, the chilling effect of the proposed offence may drive that speech offline or underground. Law enforcement and security agencies will have a far more difficult time conducting investigations and disrupting threats.

Endorsing acts of terror may be upsetting to some, and repulsive to many. But freedom of expression is what creates a democratic society, in which we can debate the merits of ideas – even those that as individuals we might find deeply offensive. A democracy is based on the premise that individual citizens have the capacity to govern themselves, to understand and evaluate different perspectives with which they are confronted, to deliberate their merits, and to ultimately decide which viewpoints to adopt, and which to discard.

Accordingly, we urge this Committee to reject the creation of an advocating or promoting terrorism offence in the *Criminal Code*.[9]

---

[7] As observed by Lamer, J. (as he then was) in *R. v. Smith (Edward Dewey)*, an otherwise constitutional law "cannot be salvaged by relying on the discretion of the prosecution not to apply the law in those cases where, in the opinion of the prosecution, its application would be a violation of the *Charter*." [1987] 1 SCR 1045 at 1078.

[8] *R. v. Levkovic*, 2013 SCC 25 at para. 33.

[9] Given our position on the proposed offence, we limit our submissions to s. 83.221. Nonetheless, we would agree with many of the concerns raised by Professors Roach and Forcese concerning deletion orders and customs seizures of "terrorist propaganda" (defined in the same terms as the criminalized expression in s. 83.221), as set out in Kent Roach and Craig Forcese, Bill C-51 Backgrounder #4, The Terrorism Propaganda Provisions (February 23, 2015). Available at http://ssrn.com/abstract=2568611.

4. The proposed amendments to recognizances to keep the peace relating to suspected terrorist activities or terrorist offences

Bill C-51 expands an already troubling regime of preventative arrest and detention. Currently, the *Criminal Code* permits preventative arrest in cases where there are reasonable grounds to believe that a terrorist activity *will* be carried out, and there are reasonable grounds to suspect that either arrest or imposition of a recognizance is *necessary* to prevent the carrying out of the terrorist activity. The proposed amendments seek to lower the thresholds for preventative arrest to situations where there are only reasonable grounds to believe that a terrorist activity *might* be carried out, and that the arrest or recognizance is *likely* to prevent the carrying out of the terrorist activity. "Will" to "might", "necessary" to "likely": this significantly lowers the bar on what is already a very low threshold for detaining individuals on mere suspicion of dangerousness.

If passed, Bill C-51 would also double the length of time an individual can be held in preventative detention. The proposed amendments also seek to extend the duration of recognizances for individuals who have been convicted of terrorism offences, and increases terms of imprisonment for breaches of recognizances in all instances.

When this Committee debated the reintroduction of the preventative detention provisions currently in the *Criminal Code*, we expressed serious concerns about the necessity for such sweeping powers of arrest and detention. While we continue to believe that it is preferable to charge terrorism suspects under the criminal law so that they are afforded appropriate due process protections, the fact remains that the government already has extraordinary powers at its disposal. Further expansion of this regime is simply unwarranted.

The question this Committee and all Canadians should be asking is not what additional powers should be granted to government to protect public safety, but how well existing powers are being used and whether the existing criminal law is being properly enforced. **It is our submission that this Committee should reject the proposed amendments relating to recognizances with conditions.**

5. The creation of additional powers for CSIS to "reduce" threats to the security of Canada

Bill C-51 seeks to radically redefine the role of CSIS and ignores the lessons of the McDonald Commission. CSIS was created in 1984 following a Commission of Inquiry chaired by Justice D.C. McDonald, who "subjected the country's security intelligence apparatus to almost four years of intense scrutiny and found it wanting."[10] The Commission found that the abuses committed by the RCMP in its security intelligence function were so egregious and systemic that responsibility for intelligence gathering and analysis should be removed from its remit altogether. The problem identified by the Commission was a structural one: a nation's secret intelligence service should not be situated in the same institution as its police. As a result, the RCMP Security Service was disbanded, and CSIS was established as a civilian agency whose principal functions were to engage in intelligence gathering and analysis.

In establishing CSIS as a civilian agency separate from the RCMP, Parliament recognized that security intelligence and law enforcement agencies play distinct and different roles when it comes to protecting national security. Accordingly, each institution was granted powers suited to its particular function, and limited in its abilities to undertake activities that went beyond its core mandate. As an intelligence service, CSIS's role is to provide intelligence information to the rest of government – it has significant powers to collect information relating to "threats to the security of Canada" for analysis, but its ability to physically act on this intelligence is limited. These limitations on CSIS's "kinetic" powers are not the result of some legislative omission when the *CSIS Act* was being drafted. Given that CSIS is permitted to conduct much of its work in secret and that the details of most of its activities will never be revealed publicly, there are sound policy reasons for limiting its abilities to engage in activities that might cross into policing.

Bill C-51, if passed, will upend that balance between security intelligence and law enforcement, and blur the carefully-drawn line between spying and policing.

---

[10] Security Intelligence Review Committee, *An Operational Audit of the Canadian Security Intelligence Service, Annual Report 1998-1999* (Ottawa: Minister of Supply and Services Canada, 1999), Statement from the Committee. Available at http://www.sirc-csars.gc.ca/anrran/1998-1999/index-eng.html.

Under the proposed s. 12.1 of the *CSIS Act*, if CSIS has "reasonable grounds to believe" that an activity constitutes a threat to the security of Canada, the Service is then permitted to "take measures, within or outside Canada, to reduce the threat". What those measures entail is undefined. The only prohibited conduct are actions that

(a) cause, intentionally or by criminal negligence, death or bodily harm to an individual;

(b) willfully attempt in any manner to obstruct, pervert or defeat the course of justice; or

(c) violate the sexual integrity of an individual.

Short of that, CSIS would have broad authority to take whatever measures it deemed "reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat." It is up to CSIS to decide whether measures are "reasonable and proportional". If any of these measures are illegal or unconstitutional, then CSIS will have to seek a judicial warrant authorizing the measures. The threshold decision to seek a warrant, however, is still up to CSIS; it may decide (correctly or not) that contemplated measures are legal and constitutional, and that decision may never by reviewed by any external body, not even SIRC, which will only conduct selective review.

These amendments to the *CSIS Act* claim to not confer on the Service "any law enforcement power". "Law enforcement", however, is a colloquial term and it is unclear what is meant by "law enforcement power" in this context. Perhaps CSIS may not have the power to "arrest" and "jail", but as the Department of Justice acknowledged during SECU's clause-by-clause review, these new disruption powers would permit CSIS to "take measures to interfere with a person's movement" – in other words, to capture and detain. The Department of Justice also noted that "rendition" or "removal to another state" are not "law enforcement powers", which means that such practices remain available to CSIS as "threat reduction" measures. As Professors Roach and Forcese observe:

> If CSIS wishes to detain or interrogate, it will do so for threat disruption purposes, not "law enforcement". The government's peculiar language

> does precisely nothing to dispel concerns about a system of CSIS "security detention" or "detention for security interrogation". Given the disturbing experience in other jurisdictions after September 11, 2001, the absence of an express, emphatic bar on detention is alarming.[11]

The range of activities authorized by this "threat reduction" power includes activities we traditionally think of as belonging to the police – detaining and holding individuals; interrogating them while in detention. Accordingly, we would say that despite the assertion that CSIS is not being granted "law enforcement" powers, it is clear that the new "threat reduction" power is, for all

intents and purposes, a policing power. It is a policing power made extraordinarily broad by virtue of the expansive definition of "threats to the security of Canada" contained in s. 2 of the *CSIS Act* – a definition that was constructed to set out the mandate of an agency responsible for collecting and evaluating information, not a policing authority. It is a policing power made dangerous given the secrecy that accompanies national security activities – rights violations may be more difficult to detect, and once detected, more difficult to remedy. And it is a power that seems wholly unnecessary – government has provided little evidence for why this expanded power should be granted to CSIS or why CSIS should have any policing powers at all.

That a judicial warrant is required before CSIS can undertake activity that violates Canadian law or the *Charter of Rights and Freedoms* is of no comfort. As a threshold matter, CSIS has a worrying pattern of breaching its duty of candour when it comes to *ex parte* processes. As noted in SIRC's most recent annual report:

> In two reviews, SIRC encountered significant delays in receiving requested documentation and had to press the Service to obtain complete and consistent answers to several questions. With effort, SIRC was eventually provided all the relevant information it required to carry out and complete its reviews, but these difficulties and delays caused the Committee concern.
>
> SIRC encountered similar disclosure difficulties in the investigation of

[11] Kent Roach and Craig Forcese, "The government has not made its case for C-51", *The Globe and Mail* (March 29, 2015). Available at www.theglobeandmail.com/globe-debate/the-government-has-not-made-its-case-for-c-51/article23678195/.

> two complaints. In one investigation, SIRC found that it had been seriously misled by CSIS and that CSIS had violated its duty of candour during *ex parte* proceedings by not proactively disclosing in its evidence its rejection of the reliability of a source of information. In a second complaint report, SIRC was critical of CSIS for failing to proactively highlight a highly relevant document. SIRC reminded CSIS that its disclosure obligations went beyond producing a large quantity of documents for SIRC's review and included the duty to proactively present the most relevant pieces of evidence before any presiding Member.[12]

The Federal Court of Canada similarly held that CSIS had breached its duty of candour when applying for a warrant to engage in foreign investigations of Canadians overseas under section 21 of the *CSIS Act*.[13] The Federal Court of Appeal affirmed that ruling.[14] Likewise, security certificate proceedings over the past decade have revealed instances of CSIS engaging in conduct that should raise concerns about its commitment to candour before the courts, such as attempting to justify security certificates on outdated and sometimes contradictory intelligence, or on sources of dubious reliability, such as Wikipedia and a text that "is considered fiction by scholars."[15]

More fundamentally concerning, however, is the proposition that Canada's courts should be tasked with authorizing measures that "will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms*". In the ordinary course, judicial warrants are issued to prevent *Charter* violations, not to authorize them. When a court issues a search warrant, the warrant transforms the search from a presumptively "unreasonable search" (which would violate the s. 8 protection against unreasonable search and seizure) to a "reasonable search". But that logic can only be applied in the context of qualified rights, such as the s. 8 guarantee, which guards only against "unreasonable search and seizure", not all search and seizure. As Professors Roach and Forcese point out, there is no

---

[12] Security Intelligence Review Committee, *Lifting the Shroud of Secrecy: Thirty Years of Intelligence Accountability, Annual Report 2013-2014* (Ottawa: Public Works and Government Services Canada, 2014) at 3 (emphasis added).
[13] *X (Re)*, 2013 FC 1275 at para. 118.
[14] *X (Re)*, 2014 FCA 249.
[15] *Almrei (Re)*, 2009 FC 1263 at paras. 194-199, 367.

concept of "reasonable" cruel and unusual punishment, no warrant-based qualifier attached to fundamental rights such as freedom of speech, freedom of association, freedom of religion.[16] This proposed warrant power profoundly misconstrues the role of the court in our constitutional system.

The *Charter* guarantees us our fundamental rights and freedoms. It is part of our constitutional law, and as such, is part of our basic law. The role of the court in our constitutional system is to ensure that both the executive and the legislature act in accordance with the law. To ask the court to authorize constitutional violations is simply offensive to the rule of law, and Canadian courts should not be asked to authorize violations of fundamental rights.

With respect, we disagree with the interpretation offered by the Department of Justice as to how this proposed warrant power would function. In his answers to questions from members of SECU during its clause-by-clause review, a senior lawyer from the National Security Law branch stated as follows:

> The suggestion that the Bill is designed to actually have a judge violate the *Charter* or be co-opted into violating the *Charter* … that is not what the Bill does. What the Bill does is precisely the opposite. It puts the judge in the position of deciding whether or not the *Charter* would be violated by the proposed measure. If it would be violated, that is the end of the matter. No one, including the judge, can authorize the measure.
>
> …
>
> The judge in fact is being put in precisely the position of looking at the facts of a particular case and determining whether or not the rights that are at issue are reasonably restricted. That is precisely one of the functions allowed a judge under the *Charter*. Section 1 provides for that determination and that's what the Bill in fact provides for.

We are not alone in disagreeing with the Department of Justice's interpretation of

---

[16] Kent Roach and Craig Forcese, Bill C-51 Backgrounder #2, The Canadian Security Intelligence Service's Proposed Power to "Reduce" Security Threats through Conduct that May Violate the Law and Charter (February 12, 2015) at 23. Available at http://ssrn.com/abstract=2564272.

the court's role in this proposed warrant regime, and this difference in interpretation should not be dismissed simply as a lawyerly dispute over the meaning of language. There should be absolutely no doubt as to whether the proposed warrant regime would permit unconstitutional state action. If it is indeed the case that no warrant can be obtained for "threat reduction" measures which would violate the *Charter*, then that should be clear in the legislative language.

Even accepting the Department of Justice's position that the proposed warrant regime only requires a court to conduct an *Oakes*-type analysis under s. 1 of the

Charter, we agree with Professors Roach and Forcese that confidential and *ex parte* warrant application proceedings are no place to conduct a meaningful s. 1 analysis.[17]

This expansion of CSIS powers is unprincipled, unwise and unnecessary. We urge the Committee to reject these amendments to the *CSIS Act*. Over the past decade, we have seen the effects of an approach to national security that at best, privileges bare legality, and at worst, descends into illegality. The consequences for the rule of law and human rights have been profound. Meanwhile, it remains an open question whether the "gloves off" approach to national security has made Canada or any of our allies any safer.

6. Increased restrictions on access to information by special advocates in security certificate proceedings under IRPA

The special advocate system in IRPA was created in response to a constitutional infirmity identified by the Supreme Court of Canada in *Charkaoui v. Canada (Citizenship and Immigration)*[18]: the government cannot rely on secret evidence in security certificate proceedings without providing some way for the named person to know the case to be met, and a procedure by which the evidence could be tested. As security-cleared counsel, special advocates are permitted to review *all* the information put before the judge. The special advocate must have full access to this information, including sensitive or classified information relating to national security; otherwise, the entire purpose of appointing security-cleared counsel in these proceedings would be frustrated.

---

[17] *Id.* at 24 to 26.
[18] 2007 SCC 9.

Bill C-51, however, seeks to limit the scope of materials produced to special advocates in security certificate proceedings. Under the proposed amendments, the government may seek the judge's permission to withhold from disclosure information that does not allow the named person "to be reasonably informed of the case made by the Minister" – in other words, information that is not strictly relevant to the security certificate. The proposed amendments go on to direct the judge to "not base a decision on information that the Minister is exempted from providing to the special advocate".

It is difficult to conceive what sort of information is being exempted – by definition, it is neither relevant to the government's case against the named person, nor is it information to be considered by the judge in determining whether the certificate is reasonable. It begs the question of why this information is being placed before the judge at all, and leads us to conclude that this class of information may be so problematic that rather than being exempted from disclosure, it *must* be made available to special advocates to review and potentially challenge.

It is our submission that the Committee should reject the proposed amendments to increase restrictions on access to information by special advocates in security certificate proceedings under IRPA.

Conclusion

Bill C-51 proposes radical changes to Canadian law and to Canada's national security apparatus. In these submissions, we have focused on our primary concerns with this omnibus bill, though there are other provisions which also trouble us, such as amendments to the *Criminal Code* to permit closed hearings and amendments to IRPA concerning appeals of disclosure decisions. Bill C-51 demands serious and careful consideration. We hope that these submissions will assist the Committee in its deliberations.

APPENDIX B

Notes for Presentation to the Public Safety Committee's Hearings on the National Security Framework

Oct. 17, 2016

Micheal Vonn, BCCLA

My name is Micheal Vonn and I am the Policy Director of the British Columbia Civil Liberties Association. We thank the Committee for its invitation.

The BCCLA is on record as calling for the complete repeal of "Bill C-51" and we have views on almost every aspect of the national security framework.

However, for my prepared remarks, I wish to make a substantive contribution to your deliberations on a topic that is getting surprisingly little airtime, given its importance and that is the new Security of Canada Information Sharing Act. The unprecedented expansion of surveillance powers in this Act, along with the controversial new CSIS threat disruption powers, were the main points of opposition of the thousands of citizens who took to the streets to protest the introduction of Bill C-51.

My discussion of the Information Sharing Act will focus on our new understanding of what is happening with the collection of datasets of personal information in the security intelligence sphere. If time permits, or perhaps during questions, I would be very pleased to unpack the ramifications of the Act in fuller detail.

But it is critical that this discussion be squarely set within the recent findings of unlawful data collection within the Five Eyes.

You will doubtless have seen today's headlines from the UK that the Investigatory Powers Tribunal has ruled that British security agencies have secretly and unlawfully collected massive volumes of personal data in breach of article 8 of the European Convention of Human Rights and that this unlawful activity has been ongoing, in some cases for a decade, in some cases close to two.

The illegal data holdings include bulk personal datasets which might include medical and tax records, individual biographical details, commercial and financial activities, communication and travel data.

The ruling confirms that for over a decade UK security services unlawfully concealed both the extent of their surveillance capabilities and that innocent people across the country have been spied upon.

This we learn today about our partner in our intelligence alliance. And it has an eerie echo of what we learned only a few weeks ago about our own, comparable intelligence data holdings.

Granted, you wouldn't have read about in the newspaper. The media coverage of SIRC's just released annual report was very focused on the review of the new threat disruption powers, which is by no means a surprise. However, largely unexplored in the public discourse was the report of SIRC's first examination into the CSIS data acquisition program, including bulk datasets. That report is an extremely damning one, very much in keeping with the situation as recently disclosed in the UK.

Unlawful data collection

SIRC advises that within CSIS's own data classifications, there are two types of datasets, one that is "referential" which on the argument that they are openly sourced and publicly available, CSIS says are not "collected" under the authority of s. 12 of the CSIS Act and therefore have to meet no standard of collection. The second type are the non-referential datasets, which CSIS considers are "collected" under the authority of the CSIS Act, so must meet the collection threshold of "strictly necessary".

Despite its characteristically calm and measured tone, what SIRC has to report on this matter is extremely alarming. Bottom line: SIRC does not agree that all the "publicly available" "openly sourced" data is in fact, publicly available and openly sourced, so there are definitely red flags in that category. But more deeply troubling, as regards the datasets that clearly fall under the requirement for 'strict necessity': "SIRC found no evidence to indicate that CSIS had appropriately considered the threshold as required in the CSIS Act."

No evidence of appropriate consideration of the applicable standard to bulk data collection of private information. It is simply impossible to read this as indicating anything other than contempt for the need to abide by the applicable law in this arena. This is so serious a matter that SIRC called for the immediate halt to the acquisition of bulk datasets until there can be a system to confirm compliance with the law.

This, then, is the situation -- one completely unmoored from the legal requirements in the CSIS Act -- to which we add the near free-for-all of the Information Sharing Act's powers.

You will recall that the Information Sharing Act applies to national security concerns defined so broadly that the definition had never before been seen in Canadian law. It constitutes a bar so low that there is hardly anything cannot be argued as being within its purview. It spans far beyond public safety into ordinary public life, encompassing everything from the administration of justice to the economic or financial stability of Canada.

There is no need under this legislation for individualized suspicion as a basis for information sharing and no impediment to entire databases of personal information being disclosed on the grounds that it may be "relevant" to an institution's mandate to detect, identify, analyze, prevent, investigate or disrupt an activity that undermines the security of Canada – again, as defined so broadly in the Act as to encompass huge swathes of ordinary public life. It is difficult to image a database held by a federal agency that couldn't be argued for on such grounds.

And perhaps, it was thought that a mechanism to protect against inappropriate data collection would exist by virtue of the CSIS Act, in that CSIS would unable to retain and use such vast data holdings unless they fell within the legal standard it is to apply to its data collection. Only we've just been told in no uncertain terms, that those legal standards are being ignored. And it is anyone's guess, for how long that situation has existed.

Further, we need to keep alive to the fact that there was never a compelling case for the legislation in the first place. In their recent response to the government's Green Paper, Professors Roach and Forcese cite a 2014CSIS briefing note that set out some concerns about a lack of clarity with respect to sharing information for national security purposes.

The briefing note did not call for the wholesale re-visioning of information sharing to address this concern about clarity, but rather suggested that "With appropriate direction and framework in place, significant improvements are possible to encourage information sharing for national security purposes, on the basis of existing legislative authorities."

Instead of the careful and measured approach called for, legislation of monumental overbreadth was enacted, which compounded the lack of clarity and paved the way for a massive increase in already illegal data holdings by security intelligence.

The Act is so far from hitting the mark of what is needful for national security that as Roach and Forcese note: "The Act allows for the government to share just about everything while it rejects the Air India commission's recommendation that CSIS must share intelligence about terrorist offences, if not to the police then to someone who is in charge and who can take responsibility for the proper use of the information."

The security benefits of the approach that has been adopted are at best entirely speculative and fail to address long-standing concerns and at worst, undermine rather than enhance effectiveness.