

# SUBMISSION TO THE STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY

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

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

### **Executive Summary**

Page 1/21

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.

Page 2/21

- 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.

Page 3/21 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

Page 4/21

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

Like Professors Roach and Forcese, we believe that limiting Canada's security interest only to *unlawful* advocacy, protest, dissent and artistic expression is not much of a limit at all. Unlawful does not necessarily mean "criminal", and an unlawful protest may simply mean a gathering without a proper permit. Moreover, given that government institutions are permitted to share information

<sup>&</sup>lt;sup>1</sup> 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.

for the purpose of detecting, identifying, analyzing, preventing, investigating, or disrupting any "activities that undermine the security of Canada", even information about lawful expressive activity can be subject to this proposed regime. After all, further identification, analysis, or investigation may be necessary to determine whether a protest is lawful. We discuss the information sharing provisions further below, but when the proposed *Act* is taken together as a whole, it is apparent that its logic is quite circular.

Page 5/21

Many of our colleagues have already raised concerns that activities undermining the security of Canada could include unlawful strikes where essential services are involved, or protests in favour of Quebec separatism that take place without proper permits. They can include the actions of environmental rights activists protesting pipeline projects, or blockades undertaken by Indigenous peoples, considered unlawful even though they may be expressions of Indigenous law and constitutionally protected. Consider as well the following situation. A group of individuals wish to protest Russia's involvement in the armed conflict in Ukraine. It is a spur-of-the-moment activity, so no permit was obtained. It is an unlawful protest. Does it undermine the security of another state? Russia might very well say it does, and it has been known to retaliate against Canadian interests. Last year, for example, it responded to Canadian sanctions by imposing a travel ban on a number of Canadian public officials. It is at least conceivable that such a protest would fall within the definition of "an activity undermining the security of Canada", given the breadth of its scope.

Government may say: but of course this is not the sort of activity we would consider to be a threat to Canadian security, and government institutions will use their judgment and discretion to ensure that they are only using powers under the *Act* to address "true" security concerns. Such an approach, however, politicizes what should be an objective assessment of risk to public safety and security. What constitutes a "true" security concern becomes subjective, and for the politically active, whether their conduct would be considered as undermining the security of Canada might turn on whether their cause is politically popular and in line with the views of the government in power. This is dangerous for freedom of expression and the right to dissent. A better approach would be the one contained in the *Criminal Code*, which explicitly exempts from the definition of "terrorist activity" *all* "advocacy, protest, dissent or stoppage of work"

regardless of its legality, so long as it does not endanger life.<sup>2</sup>

Moreover, recent examples 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."

Page 6/21

Finally, we have serious concerns that the radically expansive concept of security contained in the proposed *Act* is apt 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

<sup>&</sup>lt;sup>2</sup> See Criminal Code, s. 83.01(I)(b)(ii)(E).

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.

Page 7/21

As wide-ranging as that may seem already, the proposed *Act* does not simply limit information sharing to the scheduled institutions. Section 6 goes on to permit any receiving agency to further disseminate information "to any person, for any purpose", so long as it is "in accordance with law". But as Professors Roach and Forcese have observed, 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.<sup>3</sup> 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 to "any person, for any purpose", 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

<sup>&</sup>lt;sup>3</sup> Backgrounder #3 at 14.

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, but 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

Page 8/21

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 informationsharing 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.

Page 9/21

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. 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.

Page 10/21

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 are 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.<sup>4</sup>

<sup>&</sup>lt;sup>4</sup> 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

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 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*.

Page 11/21

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 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.

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.

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.

Page 12/21

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.<sup>5</sup>

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

<sup>&</sup>lt;sup>5</sup> Latif v. Holder, 969 F.Supp. 2d 1293 (D. Or. 2013).

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.

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

Page 13/21

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 openended 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 potentially infinite number of offences."

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

<sup>&</sup>lt;sup>6</sup> 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.

"threats of violence".7

What this new 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 impugned speech.

Page 14/21

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. It is a foundational principle of criminal law that "prohibited conduct must be fixed and knowable in advance". 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

<sup>&</sup>lt;sup>7</sup> R. v. Khawaja, 2012 SCC 69 at para. 73.

<sup>&</sup>lt;sup>8</sup> 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.

<sup>&</sup>lt;sup>9</sup> R. v. Levkovic, 2013 SCC 25 at para. 33.

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*.<sup>10</sup>

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

Page 15/21

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

<sup>&</sup>lt;sup>10</sup> 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.

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.

Page 16/21

# 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." 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

<sup>&</sup>lt;sup>11</sup> 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.

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.

Page 17/21

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. 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.

This "threat reduction" power is 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.

Page 18/21

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 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.<sup>12</sup>

The Federal Court of Canada similarly held that CSIS had breached its duty of

<sup>&</sup>lt;sup>12</sup> 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).

candour when applying for a warrant to engage in foreign investigations of Canadians overseas under section 21 of the *CSIS Act*.<sup>13</sup> The Federal Court of Appeal affirmed that ruling.<sup>14</sup> 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." <sup>15</sup>

Page 19/21

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 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. 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.

<sup>&</sup>lt;sup>13</sup> X (Re), 2013 FC 1275 at para. 118.

<sup>&</sup>lt;sup>14</sup> X (Re), 2014 FCA 249.

<sup>&</sup>lt;sup>15</sup> Almrei (Re), 2009 FC 1263 at paras. 194-199, 367.

<sup>&</sup>lt;sup>16</sup> 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.

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. <u>Increased restrictions on access to information by special advocates in security certificate proceedings under IRPA</u>

Page 20/21

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*)<sup>17</sup>: 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.

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

-

<sup>&</sup>lt;sup>17</sup> 2007 SCC 9.

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**

Page 21/21

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.