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