January 30, 2018

Written Submissions of the British Columbia Civil Liberties Association ("BCCLA") to the Standing Committee on Public Safety and National Security regarding Bill C-59, *An Act respecting national security matters*

Executive Summary

In this brief, the BCCLA sets out its chief concerns with Bill C-59, *An Act respecting national security matters*.

1. Threat disruption activities of the Canadian Security Intelligence Service ("CSIS")

Allowing CSIS to engage in threat disruption is inherently dangerous given that rights violations may be more difficult to detect, and once detected, more difficult to remedy than in the context of these activities conducted by law enforcement. C-59's revised approach to CSIS threat reduction activities does not adequately address these dangers.

If these powers are to be retained, there should be express, statutory language stating that warrants for CSIS to undertake threat disruption activities are to be granted only where CSIS can demonstrate that it is better situated than law enforcement to conduct the activities.

2. Bulk data collection by CSIS

C-59 does not appropriately constrain bulk data collection by CSIS, an activity that constitutes mass surveillance of Canadians. The provisions on bulk data collection by CSIS should be revised so that collection occurs within (and not as an exception to) the *Canadian Security Intelligence Service Act* ("*CSIS Act")* s. 12 standard of "strict necessity" for data collection.

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

We recommend:

- An appropriate definition of "publically available datasets" which expressly excludes purchased data and any data in which an individual may have a reasonable expectation of privacy; and

- An appropriate standard for collection of "Canadian datasets" such as the three-part test proposed by the Security Intelligence Review Committee ("SIRC") of 1) clear connection to a threat to the security of Canada, 2) no less intrusive means available, and 3) objective assessment of intelligence value.

3. Authorizations for Communications Security Establishment ("CSE") bulk data collection

Bulk data collection by CSE incidentally collects information about Canadians and persons in Canada, including their metadata. C-59 proposes that bulk data collection for foreign intelligence and cybersecurity activities be subject to a new process of ministerial authorization plus vetting by an Intelligence Commissioner to ensure the reasonableness of the authorization if the activity authorized would otherwise contravene an Act of Parliament. There is considerable concern that this "trigger" for mandating approval by the Intelligence Commissioner is under-inclusive.

Current proposals for a more expansive trigger present problems of interpretation. The BCCLA's position is that the best remedy for this problem is readily achieved by having all the very small number of ministerial authorizations subject to the same, uniform process of vetting by the Intelligence Commissioner.

4. Overly expansive powers for CSE to collect "publically available information".

We recommend that the definition of "publically available information" in the proposed *Communications Security Establishment Act* ("*CSE Act*") be revised to expressly exclude information that has been published or broadcast to only a selected audience and to specify that information purchased must have been legally obtained and created by the vendor.

5. CSE active cyber operations

There is an inherent problem with tasking Canada's cyber security operatives with (also) exploiting security vulnerabilities. We recommend that an active cyber operations mandate not be considered until and unless the vast array of problems identified in various submissions regarding CSE's active cyber operations are studied and remedied.

6. *Secure Air Travel Act*

We continue to hold the position that the *Secure Air Travel Act* should be repealed in its entirety. In our view, where warranted, travel bans should be imposed pursuant to a court order and not as a result of discretionary executive decision-making.

If the *Secure Air Travel Act* is retained, C-59 does not go far enough to remedy the deficiencies of the scheme. It remains a scheme in which travellers have no concrete way of knowing whether they are on the '"no-fly list", reasons for listing can still be kept largely secret, and administrative recourse is still insufficient. Further, individuals on the '"slow-fly list" (subjected to enhanced security scrutiny) have no recourse mechanism whatsoever.

We call for a proper redress system for people who are ensnared in the *Secure Air Travel Act* scheme but are "false positives" (e.g. same/similar name as a listed individual). Recent calculations estimate over 100,000 Canadians could be affected as potential false positives.

We recommend:

- That the basis for the decision to list an individual as a person who is prohibited from flying be increased from the troubling low threshold of "reasonable grounds to suspect" to "reasonable grounds to believe";

- That individuals who are placed on the "no-fly list" be given notice of the fact so they can seek administrative recourse without first having to be barred from a flight. We recommend that individuals who are placed on the "slow fly list" be able to be informed of this fact, and that a mechanism to challenge the listing exist for this list as well;

- That administrative recourse be available to all affected persons and that the 60 day timeframe for their right to file an application start from the day upon which they find out their status as a listed person (instead of the current starting point of when they are denied transportation). The timeframe for the minister to make a decision needs to be reduced and the "clock" of 120 days shouldn't restart upon the Minister providing notice of insufficient information;

- Full disclosure of relevant information to the court hearing a listed person's appeal and expressly provide that this must include exculpatory information in the possession of the government; and

- Provision for the appointment of a Special Advocate to assist individuals appealing their listed status. Without access to a Special Advocate, there can be no effective adversarial challenge in the appeal process.

7. *Security of Canada Information Disclosure Act* ("*SCIDA*")

We maintain that *SCIDA* is fundamentally flawed and should be repealed.

If *SCIDA* is retained, we recommend:

- Replacing the definition of "activity that undermines the security of Canada" with the narrower definition of "threats to the security of Canada" as used in the *CSIS Act*;

- That receipt of information be governed by a standard of necessity and proportionality, not mere relevancy;

- Providing clear rules that govern recipient institution's retention, correction and destruction of information and the addition of record keeping and reporting obligations on institutions that receive information under the *SCIDA*;

- The repeal of the "no presumption" provisions that may be used 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; and

- Clarifying the ambiguity regarding the role of the Privacy Commissioner and the application of the *Privacy Act* and giving the Privacy Commissioner the legal authorities required to participate in review and oversight of information sharing for national security purposes.

8. Torture-tainted information

Canada should have a clear and total prohibition on the use or sharing of information likely to be derived from torture or lead to torture and this prohibition should be grounded in statute so the rules are transparent and subject to parliamentary scrutiny.

We recommend that C-59 be amended to include this prohibition.

Introduction

The 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 on the principles which protect individual rights and freedoms, and have played an important and prominent role in 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.

Bill C-59 is a complex, inter-related omnibus bill. We appreciate that there have been submissions on this bill that overview a very broad range of concerns and we do echo many of the particularized items that have been raised. However, our submission does not canvas the bill in an item-by-item fashion, but rather, takes a thematic approach to addressing the matters which constitute our chief concerns.

Canadian Security Intelligence Service ("CSIS")

a) Threat reduction powers

In empowering CSIS to undertake active measures for threat reduction, *the Anti-terrorism Act, 2015* ("ATA, 2015") upended the balance between security intelligence and law enforcement that reflected the sound policy decisions that flowed from the lessons of the McDonald Commission. It continues to be the BCCLA's position that this expansion of CSIS powers is unprincipled, unwise and unnecessary.

The changes to CSIS's threat disruption powers that are proposed in C-59 are obviously an improvement over the constitutionally-problematic scheme enacted in the ATA, 2015. However, under C-59, CSIS would continue to be granted powers which are essentially policing powers and these powers are 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. The revised approach under C-59, which appears to aim at bare legality, does not adequately address these dangers.

If these powers are to be retained, there should be express, statutory language stating that warrants for CSIS to undertake threat disruption activities are to be granted only where CSIS can demonstrate that it is better situated than law enforcement to conduct the activities.

b) CSIS bulk data collection

The BCCLA has been concerned that the government's response to the CSIS bulk data collection scandals would be to simply empower the agency to do what it had previously done unlawfully without having a meaningful democratic debate about mass data acquisition in the context of national security.

We appreciate that having bulk data collection squarely on a legislative footing does improve transparency, but we are deeply concerned about the thresholds that are proposed in C-59 and further concerned that this critically important topic is receiving insufficient attention in the context of such a large omnibus bill.

Within the last two years, the SIRC completed its first ever audit of the bulk data collection programs of CSIS. SIRC is of the view that appropriate bulk data acquisition by CSIS can occur within the *CSIS Act* s. 12 standard of "strict necessity" for data collection. In our view, it is hard to imagine a body that would be in a better position to assess this, both from the perspective of accountability and respect for the rule of law and from the perspective of the operational needs of CSIS.

SIRC's proposal for standards and criteria for bulk data collection is a three-part test:

1) Clear Connection to a Threat to the Security of Canada: a clear connection to a threat to the security of Canada as defined in section 2 of the *CSIS Act* must be established;

2) No Less Intrusive Means Available: it must be established that less intrusive means that would satisfy the intelligence requirements are not available as an alternative to bulk collection, consistent with the principle of proportionality;

3) Objective Assessment of Intelligence Value: if there is no reasonable alternative to bulk collection, CSIS needs to provide an objective assessment of how closely connected the bulk information is to intelligence value; the broader the intended collection, the most strictly CSIS must establish the connection between the bulk information and the threat-related intelligence.

The standards for bulk data collection as set out in C-59 are woefully below the standard proposed by SIRC.

The undefined "publically available" datasets

C-59 allows CSIS to collect "publically available" datasets (with no actual definition of that term) on the basis of a bare "relevance" standard. In its 2016 annual report, SIRC provided insight into what CSIS had termed its "referential" datasets, which were said to be openly sourced and publically available. SIRC found that these bulk data holdings included data that was not openly sourced and publically available. Thus the only record of accountability on "publically available" information collection provides no reason to be confident of constraint and accuracy in such collection.

We echo the recommendation of the Canadian Civil Liberties Association in calling for "publically available datasets" to be defined clearly and narrowly to expressly exclude purchased data and any data in which an individual may have a reasonable expectation of privacy.

The "Canadian Datasets"

With respect to Canadian Datasets, which are defined as datasets that contain personal information expressly acknowledged as *not* directly and immediately relating to activities threatening the security of Canada, the test for their acquisition is simply that the results of querying or exploiting this personal information could be "relevant" and this assessment must be "reasonable".

It may be argued that this vastly wide scope for bulk collection is at least mitigated by the requirement for judicial authorization for retention of the Canadian Datasets. But rather than significant gate-keeping, this authorization simply compounds the effect of all of the very low standards that lead up to it. In this scheme, personal information that does not directly and immediately relate to threats to the security of Canada is allowed to be collected if it "could be relevant", this assessment must be "reasonable" and the judge decides whether the dataset can be retained on the standard that is "likely to assist".

These then are the thresholds for what most Canadians would term "mass surveillance" and which we believe most Canadians would reject as shockingly low standards. Thus a genuine opportunity to meaningfully shape these surveillance practices is being squandered. These standards represent a massive erosion of privacy protection from the "strict necessity" standard, especially when juxtaposed with the criteria that SIRC proposed.

Our recommendation is that C-59 provisions relating to CSIS bulk data acquisition be revised to be expressly *within* the *CSIS Act* s. 12 strict necessity standard and not an exception to the strict necessity standard. SIRC has made a proposal that it views as implicitly principled and workable. We are not aware of any case made by the government for why Canadians should be subjected to bulk data collection of their personal information on the shockingly low standards contained in C-59, when a much more carefully tailored and privacy protective standard has been outlined by SIRC.

Communications Security Establishment ("CSE")

a) CSE bulk data collection

C-59 would enact the *CSE Act* under which the CSE would have five mandates: 1) foreign intelligence, 2) cybersecurity and information assurance, 3) defensive cyber operations, 4) active (offensive) cyber operations, and 5) technical and operational assistance.

The BCCLA has a particular recommendation with respect to the thresholds for authorization for CSE data collection.

Section 23 of the proposed *CSE Act* requires that the CSE's own (non-assistance) mandates not be directed at Canadians or persons in Canada. Nevertheless, it is well established and conceded that the information of Canadians and persons in Canada is collected by the CSE because some collection, and by no means insignificant collection, is unavoidable due to the complexity of communication networks. Thus Canadians' information is collected "incidentally" or "unavoidably".

Part of the new regime proposed for protection of Canadians' privacy interests is to require CSE to seek a ministerial authorization that is then approved by the Intelligence Commissioner. The trigger that initiates this process of authorization in conjunction with intelligence commissioner vetting is where the CSE's activities would otherwise "contravene any other Act of Parliament".

We agree with the submission of others, including Professor Craig Forcese, that this trigger is under-inclusive. As Professor Forcese notes, there is concern that the proposed threshold would not ensure that the authorization process would, for example, be initiated for activities that incidentally collect Canadians' metadata, which is obviously of critical importance.

However, we believe that the proposal for a more expansive trigger, in which the authorization process is required for activities that would otherwise contravene any other Act of Parliament *or* "involve the acquisition of information in which a Canadian or person in Canada has a reasonable expectation of privacy", is problematic.

Simply put, the question of what precisely attracts a reasonable expectation of privacy is typically the central dispute in almost any emergent privacy issue you can name. This is not a standard that should be adjudicated internally by the CSE. We know, not least from years of reports from the CSE Commissioner, that disputes over interpretation of legal standards and definitions has been an on-going concern. National security activities in general are plagued with the "secret laws" problem of having words in a statute or directive interpreted in sometimes obscure and deeply troubling ways and this fact remaining undiscovered for years. So a trigger that involves such a colourable definition is inherently problematic.

However, we read the latest CSE Commissioner's report as indicating that CSE has conducted its signals intelligence activities under just 3 Ministerial Authorizations since 2015. It appears that

these authorizations tend to authorize a broad sphere of activities. Our understanding of the frequency and scope of "incidental collection" suggests that most or all authorized activities are apt to implicate Canadians' data. In other words, there are only a very small number of authorizations and almost all or all of them are apt to include information in which Canadians or persons in Canada would likely have a reasonable expectation of privacy.

In our view, in order to ensure that the authorization process proposed does examine, and therefore bring accountability, to all the arenas that involve Canadians' reasonable expectation of privacy, there must be one uniform process whereby all classes of activities undertaken by CSE (except in its technical and operational assistance mandate) are subject to authorizations which are vetted by the Intelligence Commissioner. Every indication as to current number of CSE authorizations suggests that this process is entirely feasible and would not involve an undue administrative burden.

We then recommend that the question of threshold be resolved by eliminating the need for a threshold and ensuring that every class of activities authorized outside of the assistance mandate are subject to the accountability procedure that includes vetting by the Intelligence Commissioner.

We further recommend that the definition of "publically available information" in the *CSE Act* be revised to expressly exclude information that has been published or broadcast to only a selected audience and that specifies that information purchased must have been legally obtained and legally created by the vendor.

b) CSE active cyber operations

The BCCLA shares the concerns that have been voiced about the expansion of the CSE's mandate to include "active cyber operations". We concur with the view that there is an inherent problem with tasking your cyber security operatives with exploiting security vulnerabilities.

We recommend that an active cyber operations mandate not be considered until the vast array of problems identified in various submissions are studied and remedied.

Secure Air Travel Act

We continue to hold the position that the *Secure Air Travel Act* should be repealed in its entirety due to our doubts about 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. Where warranted, travel bans should be imposed pursuant to a court order and not as a result of discretionary executive decision-making.

Even if no-fly lists do have an effect on aviation security, the system under the *Secure Air Travel Act* is deeply flawed. It 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, administrative recourse is insufficient and where the judicial process for reviewing delisting applications can be held in secret. This is a dangerous lack of due process.

The amendments proposed by C-59 do not go far enough to remedy the deficiencies in the scheme. We have a number of recommendations for how the legislation should be changed to better protect the rights of individuals affected by it.

a) Redress system for false positives

We join a chorus of people and organizations demanding that a proper redress system be established for people who are ensnared in the administration of the *Secure Air Travel Act* due to similarities between their identity and those of listed individuals. Recent conservative estimates are that over 100,000 Canadians are potential false positives, based on the names of falsely flagged individuals that are known.

This is a shockingly high number of affected individuals. Even if we accept that some false positives are unavoidable, it is unconscionable that a person's travel can be disrupted and no one is obliged to tell them why. Each person who is falsely identified as a result of this statutory regime should be immediately informed of their predicament and have access to a timely and effective form of redress if they are flagged improperly.

We believe that the operation of the *Secure Air Travel Act* should be suspended until the government develops an adequate mechanism to assist people falsely identified as being listed. It is shameful that innocent people continue to face real hardships that hinder their mobility rights while the government neglects to develop the law and technology required to provide even basic relief.

b) Increase the threshold required to list persons

It is inappropriate that such a low threshold – "reasonable grounds to suspect" - is used to infringe a person's mobility rights under this legislation. This is the lowest bar in Canadian law and merely requires that there be a possibility (and not a probability) that a person may engage in any activities at issue.

We recommend increasing the threshold for a Minister's decision to add a person to the list to "reasonable grounds to believe" that they will pursue an activity listed in section 8.

c) Remedy the lack of notice and insufficient recourse for listed persons

The lack of due process for a person who is affected by a Minister's decision or direction under this *Act* is deeply troubling. It is fundamentally unfair that a listed person can be ignorant of their status unless and until they attempt to fly, and even then the air carrier is prohibited from disclosing any information to the person about whether or not they are listed.

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 listed. If the person somehow infers that their treatment by the air carrier is the result of having been listed under this *Act*, administrative recourse is limited to those who are prevented from travelling. Those who are listed but directed for enhanced screening (and not denied transportation) are unable to apply to the Minister to have their name removed. There is no reason to deprive this class of people from seeking recourse.

We recommend that the *Secure Air Travel Act* be amended to provide procedural fairness to all individuals affected by Ministerial decisions and directions made under the *Act*. The Minister should have to provide notice to a person upon making a decision to add or remove them from the list.

d) Remedy the administrative recourse procedural deficiencies

The amendments proposed by Bill C-59 are insufficient in terms of rectifying the flawed administrative recourse mechanism available under the *Secure Air Travel Act*. When applying for a delisting, the individual knows only that they have been denied the ability to board an aircraft. They are not informed of any reasons for their listing. Their task is to prove a negative – that they are not threat to aviation safety and that they are not about to commit a terrorist offence. Currently, the Minister is given 90 days to make a decision on the application. If no decision is rendered, then the individual is deemed to remain on the list.

While we welcome the C-59 amendment to deem any lack of a ministerial decision within the time frame as a decision to delist the person (rather than maintain their listing), we are disappointed to see the proposal gives the Minister an additional 30 days to make a decision (extending the timeframe to 120 days from 90). The amendments also contemplate enabling the Minister to reset this 120 day waiting period at any point if they provide notice to the applicant that there is insufficient information to make a decision. This means that it could take up to eight months before the applicant finds out whether a decision has been made to delist them. And even then, the decision could simply be to reject the application.

We recommend that administrative recourse be available to all affected persons and that the 60 day timeframe for their right to file an application start from the day upon which they find out their status as a listed person (instead of the current starting point of when they are denied transportation). Given how disruptive listings are to a person's life, the timeframe for the Minister to make a decision needs to be reduced and the "clock" of 120 days shouldn't restart upon the Minister providing notice of insufficient information.

e) Fix the appeal process

A listed person can seek judicial review of the Minister's refusal to delist. 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 current scheme that C-59 does not propose to alter, 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.

We recommend that C-59 amend the *Secure Air Travel Air Act* to require full disclosure of relevant information to the court judicially reviewing a listing and expressly provide that this must include exculpatory information in the possession of the government.

We recommend that C-59 amend the *Secure Air Travel Act* to provide for the appointment of a Special Advocate to assist individuals appealing their listed status. The Special Advocate should have the same powers and obligations as they do when challenging security certificates. Without access to a Special Advocate, there can be no effective adversarial challenge in the appeal process.

f) Summary of recommendations regarding the *Secure Air Travel Act*

It is our submission that this Committee should recommend the repeal of *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.

Short of a repeal of the *Act*, we recommend that this Committee:

- Suspend the operation of the *Secure Air Travel Act* until it develops the technology to administer an adequate redress system;

- Replace the threshold "reasonable grounds to suspect" with "reasonable grounds to believe" in sections 8 and 15(5);

- Add an obligation for the Minister to provide notice to a person upon making a decision to add or remove them from the list, as well as when the minister makes directions for air carriers in relation to that person;

- Provide administrative recourse to all affected persons and start the 60 day timeframe for their right to file an application from the day upon which they find out their status as a listed person (instead of the current starting point of when they are denied transportation). Given how disruptive no-fly listings are to a person's life, the timeframe for the minister to make a decision needs to be reduced and the "clock" of 120 days shouldn't restart upon the Minister providing notice of insufficient information; and

- Require full disclosure of relevant information to the court judicially reviewing a listing and expressly provide that this must include exculpatory information in the possession of the government.

Security of Canada Information Disclosure Act (SCIDA)

SCIDA provides only a few changes from its predecessor the *Security of Canada Information Sharing Act*. We maintain that the information-sharing scheme in *SCIDA* is (still) fundamentally flawed and should be repealed. It is obvious that such widespread and relatively unfettered access to individuals' information by all of government 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 *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.

If there are barriers to information disclosure for national security purposes, they should be remedied through amendments to the *Privacy Act* or though the authorizing legislation for each government institution and not through *SCIDA*.

a) Overbroad scope of "activity that undermines the security of Canada"

The basic premise of the *SCIDA* is to "encourage and facilitate the disclosure of information between Government of Canada Institutions in order to protect Canada against activities that undermine the security of Canada." Two years ago we argued that the definition provided for an "activity that undermines the security of Canada" was too expansive and could lead to the unwarranted and unnecessary scrutiny into the private lives of many Canadians.

Bill C-59 does not remedy this concern. While we acknowledge that some of the amendments in this bill narrow the scope of activities under this definition, other aspects are actually broader. The "chapeau"' of the definition is being altered so that it will not just include "activities that undermine the sovereignty, security or territorial integrity of Canada or threatens the lives or the security of people in Canada" but arguably also "any individual who has a connection to Canada and is outside Canada." These additional terms are undefined which leads to an extremely wide potential interpretation by government agencies.

We are particularly concerned about the inclusion of "conduct that takes place in Canada and that undermines the security of another state" under the definition. Recall that the exception provided for "advocacy, protest, dissent or artistic expression" does not apply if these are carried out in conjunction with an activity that undermines the security of Canada. Our concern is that this will enable the government to monitor Canadians expressing themselves about foreign politics. In our view, such a threat to freedom of expression is not justified. The exception for expressive activities

should only dis-apply if carried out in conjunction with violence (using an approach analogous to the criminal offense of "terrorism").

Due to the expansive nature of this definition, we think it should be repealed and replaced with the narrower definition of "threats to the security of Canada" used in the *CSIS Act*. This recommendation echoes that of the Privacy Commissioner and the Standing Committee on Access to Information, Privacy and Ethics.

b) Necessity threshold needs to apply to the disclosure and receipt of information

When Canada's security is conceived of in terms as broad as those set out in *SCIDA*, the range of activities that could serve as justification for massive information sharing is dramatically expanded. When the aim is to identify threats (as opposed to tracking known threats), there is nothing in the existing or proposed legislation to prevent government institutions from either requesting or providing entire databases for use by any of the scheduled institutions.

While C-59 would improve upon the very low relevancy standard that currently authorizes one government institution to disclose information to another, the amended s. 5 of *SCIDA* falls short of the international standard of "necessity" that the Privacy Commissioner continues to advocate for. The amendments set the bar too low by allowing disclosure if it "will contribute to the exercise of the recipient institution's jurisdiction" and "will not affect a person's privacy interest more than is reasonably necessary."

We also agree with the Privacy Commissioner that privacy rights will not be sufficiently protected unless a standard higher than relevancy applies to the receipt of information under the *Act*. Receiving institutions should not be governed under the *Privacy Act*'s relevancy standard but rather one of necessity and proportionality.

c) Retention, correction and destruction of information by receiving institution

There is no current or proposed clear obligation on recipient institutions with respect to the retention, correction and destruction of information received under *SCIDA*. Decisions over such important matters shouldn't be left to bureaucrats to decide; well-defined rules of law are needed. The Federal Court's finding in 2016 that CSIS retained information illegally underscores this need.

The Standing Committee on Access to Information, Privacy and Ethics, after its study of *SCIDA*, specifically recommended that that regulation-making power be added to enable rules that govern the correction, deletion and retention of information. We recommend that *SCIDA* be amended to include clear rules that govern recipient institution's retention, correction and destruction of information.

d) Review of actions taken under SCIDA should extend to recipient institutions

People hesitate to share information with the government if they don't trust that it will be properly protected. It is critical that scheme provide accountability to maintain public confidence. For this reason, we welcome the record keeping requirements that C-59 will add for disclosing institutions, and the related obligation to provide a copy of such records to the National Security and Intelligence Review Agency on an annual basis.

We recommend that C-59 amend *SCIDA* to impose analogous record keeping and reporting obligations on institutions that receive information. This will assist reviewers in ascertaining whether institutions are in compliance with *SCIDA* and enable Canadians to better understand how and why their information is being shared within government.

e) "No presumption" provisions

Section 7 of the *Act* expressly sets out that the act of disclosing information does not create a presumption:

> (a) that the disclosing institution is conducting a joint investigation or decision-making process with the recipient institution and therefore has the same obligations, if any, as the recipient institution to disclose or produce information for the purposes of a proceeding; or
>
> (b) that there has been a waiver of any privilege, or of any requirement to obtain consent, for the purposes of any other disclosure of that information either in a proceeding or to an institution that is not a Government of Canada institution.

C-59 does not amend this problematic provision which can be used 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 their fair trial rights are respected, it will be up to the accused to seek it.

We recommend that Bill C-59 repeal the "no presumption" provisions that may be used 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

f) Resolve ambiguity about the application of the *Privacy Act* & role of Privacy Commissioner

It is unfortunate that Bill C-59 does not resolve the legal ambiguity and circularity introduced by *SCIDA* with respect to the *Privacy Act*. The legislation is also silent on the role of the Office of the Privacy Commissioner. While we are pleased that the National Security Intelligence Review Agency will have a mandate to review information sharing under *SCIDA*, we think it is ineffective to exclude the Privacy Commissioner from a formal oversight role.

The Standing Committee on Access to Information, Privacy and Ethics agreed that the Privacy Commissioner of Canada should have the role of overseeing how information is shared and used under *SCIDA*, and to report his or her findings to Parliament.

To resolve the legal uncertainty and to maximize the thoroughness of the review architecture, we strongly endorse the "effective review and oversight" recommendations made by Privacy Commissioner in his written submission to this Committee.

g) Summary of recommendation regarding *SCIDA*

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

Short of a repeal of the *Act,* we recommend that this Committee:

- Repeal the definition of "activity that undermines the security of Canada" and replace it with the "threats to the security of Canada" in the *CSIS Act;* or

- If the definition is not repealed and replaced, remove 2(h) from the definition of "activity that undermines the security of Canada."

- The exception provided for expressive activities in s. 2(2) should apply unless carried out in conjunction with violence;

- Amend the bill to require that disclosure of information be "necessary" to the exercise of a recipient institution's jurisdiction. The necessity standard should also apply to the receipt of the information by the receiving institution;

- Add clear rules to govern the retention, correction and destruction of information by institutions that receive information under the *Act*;

- Extend record keeping and reporting requirements to government institutions who receive information under *SCIDA*;

- Repeal the "no presumption" provisions that may be used 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;

- Clarify any ambiguity regarding the role of the Privacy Commissioner and the application of the *Privacy Act*; and

- Give the Privacy Commissioner the legal authorities required to participate in review and oversight of information sharing for national security purposes

Ministerial Directives on 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.

In 2017 the rules governing the contexts in which government institutions (e.g. CSIS, CSE, Global Affairs Canada, Department of National Defence, and Canadian Armed Forces) may exchange information with foreign entities if the information conveyed is derived from torture, or torture may result, were narrowed through Ministerial Directions.

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.

Canada should have a clear and total prohibition on the use or sharing of information likely to be derived from torture or lead to torture and this prohibition should be grounded in statute so the rules are transparent and subject to parliamentary scrutiny.

We recommend that C-59 be amended to include this prohibition.