Brief on Bill C-59, the *National Security Act, 2017*

International Civil Liberties Monitoring Group

May 2019

About the International Civil Liberties Monitoring Group (ICLMG)

The ICLMG is a national coalition of Canadian civil society organizations that was established in the aftermath of the September 2001 terrorist attacks in the United States and the adoption of the Canadian *Anti-Terrorism Act* of 2001. The coalition brings together 45 NGOs, unions, professional associations, faith groups, environmental organizations, human rights and civil liberties advocates, as well as groups representing immigrant and refugee communities in Canada.

In the context of the so-called 'war on terror,' the mandate of the ICLMG is to defend the civil liberties and human rights set out in the Canadian *Charter of Rights and Freedoms*, federal and provincial laws (such as the *Canadian Bill of Rights*, the *Canadian Human Rights Act*, provincial charters of human rights or privacy legislation), and international human rights instruments (such as the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights*, and the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*).

Since its inception, ICLMG has served as a round-table for strategic exchange — including international and North/South exchange — among organizations and communities affected by the application, internationally, of new national security ("anti-terrorist") laws. ICLMG has provided a forum for reflection, joint analysis and cooperative action in response to Canada's own anti-terrorist measures and their effects, and the risk to persons and groups flowing from the burgeoning national security state and its obsession with the control and movement of people.

Finally, further to its mandate, the ICLMG has intervened in individual cases where there have been allegations of serious violation of civil liberties and human rights. The ICLMG has also intervened to contest proposed legislation, regulations and practices that contravene the Canadian Constitution, other Canadian laws and international human rights standards.

Introduction

In 2015, the Conservative government caused uproar with Bill C-51, the *Anti-Terrorism Act, 2015*. Ostensibly in response to the killing of two members of the Canadian Armed Forces in separate events, many saw it as the government seizing an opportunity to pass national security legislation long in the works. Thousands of Canadians took to the street, and tens of thousands spoke out, denouncing both the process and the content of the bill. The ICLMG and our 45 member organizations were part of this movement to protect Canadians' civil liberties.

We were disappointed with the Liberal Party's decision at the time to vote in favour of the bill, and not promise an eventual repeal. At the same time, we were hopeful that the party's promise of fixing the worst elements of Bill C-51 would result in substantial changes.

Over the next two years, and following a change in government, we have monitored the implementation and use of the powers in the *Anti-Terrorism Act, 2015*. We have also actively participated in government consultations on what reforms are needed in our national security laws and activities, both in relation to Bill C-51 as well as more broadly.

We were buoyed by the May 2017 report from the House of Commons Standing Committee on Public Safety and National Security regarding its review of Canada's national security landscape. We also welcomed the findings of the third-party analysis of the federal National Security Green Paper consultation, which showed that the vast majority of respondents supported ICLMG's positions, favoured action to protect civil liberties and asserted that many provisions of Bill C-51 and other powers proposed in the federal Green Paper went too far.

We recognize that Bill C-59 makes efforts to move in this direction – particularly around new review and oversight bodies, as well as some changes to the criminal code. Unfortunately, it does not go far enough. Rather, we see Bill C-59 fitting into the steady progression, since the *Anti-Terrorism Act* of 2001, of expanding and enshrining significant, secretive powers in the hands of Canada's national security agencies. We do not doubt the need for security, but thoroughly believe that we cannot ensure the protection of our vital rights, and thus ensure our security, when so much is done without public scrutiny, or when it is allowed to take place outside Canada's transparent and rigorous judicial system. This is without mentioning the myriad powers which are such a violation of our rights that no degree of oversight or review can justify them.

In the following pages, we present realistic, necessary recommendations, suggestions and areas of examination that we believe will help to strengthen not just our fundamental rights, but also our security, as the two are intrinsically linked.

List of Recommendations

Part 1: National Security and Intelligence Review Agency (p. 9)

1. a) That the minimum number of members of the NSIRA be set at 5 and the maximum number be increased to 8 (in addition to the Chair).
   b) That, in addition to nomination of NSIRA members being carried out in consultation with opposition parties, the final appointment be made by a 2/3 vote in the House of Commons. (p. 9)
   c) That the membership will include people from diverse communities and multiple sectors – including those with an expertise in civil liberties and human rights. (p. 9)
2. That the NSIRA complaints mechanism be amended to apply to all national security activities, regardless of department. At a minimum, it should be modified to include both CBSA's and Global Affairs Canada's national security activities. (p. 9)
3. That a more specific requirement be added under "Public Reports" to mandate a listing of each departmental study requested, and its result. (p. 10)
4. a) That the NSIRA be granted binding recommendation powers. (p. 10)
   b) That the NSIRA's annual public reports include a mandatory follow-up and review of previous recommendations. (p. 10)
5. That the complaints investigation and reporting mechanisms be amended to ensure greater transparency and accountability; that complainants get access to all the information necessary to their case; that all representations or recommendations made during the complaints investigation process are available to complainants; and that, to the greatest degree possible, complaint findings are released to the public. (p. 11)
6. The NSIRA should be able to rule on and offer redress to complainants. (p. 12)

Part 1.1: Avoiding Complicity in Mistreatment by Foreign Entities (p. 13)

7. That the current act be replaced by legislation outlawing any use or sharing of information that will make Canada and its government agencies complicit in foreign mistreatment or torture[1] and require mandatory yearly reporting by departments on how they fulfilled this obligation. (p. 14)
8. That annual reports on adherence to directions on avoiding complicity in mistreatment by foreign entities not be subject to undue vetting. To that end, the provision allowing for their redaction based on injury to "international relations" should be removed. (p. 14)

Part 2: Intelligence Commissioner (p. 15)

1. a) That the IC be nominated by the Governor in Council, but approved by a 2/3 vote in the House of Commons. (p. 15)

[1] As we have noted here: http://iclmg.ca/new-ministerial-direction-on-avoiding-complicity-in-mistreatment-by-foreign-entities-falls-short-on-fulfilling-goal-of-preventing-the-sharing-requesting-or-use-of-information-tied-to-torture/, the most recent directives on the use and sharing of

b) That the IC be appointed on a full-time, rather than a part-time basis. (p. 15)
c) That the pool for selection should also include active superior court judges. (p. 15)

2. That the NSIRA be mandated to include a section regarding the work of the Intelligence Commissioner, including an external review of their work. (p. 15)
3. a) That the IC be able to impose conditions on approved authorizations. (p. 16)
   b) That both the approval of the IC and consent of the Minister of Foreign Affairs be required for all cyber operation authorizations. (p. 16)

Part 3: Communications Security Establishment (p. 17)

General recommendations:

A. That the Intelligence Commissioner be empowered to review all CSE activities.
B. That the government take steps to further narrow the scope of the CSE's surveillance and cyber activities overall.
C. That, to ensure accountability of the CSE, the independence and transparency of the work of the Intelligence Commissioner be strengthened and, to the greatest amount possible, the CSE's powers and authorizations be narrowly defined.

Specific recommendations:

1. That "international affairs" be removed from the Communications Security Establishment's (CSE) cyber operations mandate. (p. 17)
2. That more must be done to ensure that the CSE's activities actually cannot target or implicate Canadians or people in Canada. In particular, a warrant should be required for any activities that could implicate Canadians or people in Canada, including activities related to the CSE's technical and operational assistance to other law enforcement and intelligence agencies such as the RCMP and CSIS. (pp. 17-18)
3. That the *CSE Act* should define metadata; strongly limit its collection, use and retention; and require a warrant for metadata collection. (p. 18)
4. a) That Ministerial Authorizations of surveillance operations be restricted to a precise and narrow target.
   b) That the targeting of unselected information be removed from the *CSE Act,* or, at a minimum, that the Intelligence Commissioner be granted the powers to rule that such actions are disproportionate, and/or impose binding limits.
   c) That information collected should not be retained longer than *necessary* to fulfill the intended objective.
   d) That Ministerial Authorizations be reduced to the amount of time *necessary* to fulfill the intended objective, and any extension and changes should only be done with the examination and approval of the Intelligence Commissioner.
   e) That the Canadian government not engage in mass surveillance. Barring that, that it at a minimum questions the use of mass surveillance, and provides evidence to the public as to the effectiveness and necessity of surveillance – especially if it is approved in secret. (pp. 19-20)
5. a) That the definition of "publicly available information" be limited in application to commercially available publications and broadcast, that further restrictions be placed on any collection of such data. (pp. 18 & 21)
   b) That the CSE may only acquire, use, analyze and retain publicly available

information if such information falls within a dataset approved by the Intelligence Commissioner. (p. 21)

6. That greater restrictions be imposed on the CSE's carrying out of work in support of the *Investment Canada Act,* including limits on how information is collected, retained, analyzed and disposed of. (p. 21)
7. That incidentally acquired information can only be retained so long as it is necessary for protecting the security of people in Canada. (p. 22)
8. a) That the *CSE Act* enshrine strong privacy protections around CSE's activities into law. (p. 22)
   b) That the problematic actions of the CSE, including those revealed by Edward Snowden, be outlawed. (pp. 22-23)
9. That information gathered in order to protect information infrastructure from mischief, unauthorized use or disruption not be disclosed for any other purpose. (p. 23)
10. That, regarding designating persons for the purpose of disclosure of Canadian identifying information, the Minister of Public Safety should report such a designation and the reasons for the disclosure to either the Intelligence Commissioner or Privacy Commissioner, who may then rule on it. These reports should also be provided to the NSIRA. (p. 23)
11. a) That all arrangements with foreign countries be strongly regulated, limited and approved by the Intelligence Commissioner.
    b) That when sharing information with a foreign country, it is necessary for the Intelligence Commissioner to explicitly determine the likelihood that bodily harm – including mistreatment or torture – could be at play in any arrangement.
    c) That the Intelligence Commissioner include an analysis of what impact an authorization may have on mistreatment or torture in their written decisions. (p. 23)
12. That judges be prevented from ordering that confidentiality be respected if it hinders due process. (p. 24)
13. That the practice of the Five Eyes spying on each other, and the use of such information to skirt rules prohibiting the surveillance of Canadians or people in Canada, be outlawed. (p. 24)
14. a) That the definition of possible cyber operations be narrowed to only allowing activities that are strictly necessary to protect the security of people in Canada.
    b) That cyber operation powers be considered akin to military actions and should be discussed publicly, and that further restrictions should be placed on them, including oversight and reporting from the Intelligence Commissioner.
    c) That cyber threats not be used to expand domestic surveillance powers
    d) That the creation and use of any cyberweapons be strongly limited.
    e) That cyber security initiatives have genuine oversight and be more transparent.
    f) That cyber operations only allow defensive purposes, not offensive cyberattacks.
    g) If active cyber operations are still allowed, that they require the approval of the Intelligence Commissioner or of Parliament. (pp. 24-25)

Part 4: The *CSIS Act* (p. 28)

1. That the bill be amended to repeal CSIS' current threat reduction powers. (p. 28-32)

2. a) That collecting entire datasets be removed from the bill and CSIS' surveillance activities be only targeted to specific people and threats. (p. 33)
   b) If the collection of datasets is kept in the bill, that authorizations for Canadian datasets should be reduced from two to one year, with the possibility of requesting an extension in writing. (p. 33)
   c) That documentation of all queries of Canadian and foreign datasets (including reasons for and results) be shared with the NSIRA for review within 30 days. (p. 34)
   d) That the Federal Court have the power not only to examine the relevance of a query but also any eventual use of that query in order to ensure that ramifications of an illegal query are addressed. (p. 34)
   e) That authorizations for foreign datasets be reduced from five to one year with the possibility of extension for one more year granted only by the Intelligence Commissioner. (p. 34)
   f) That querying datasets for foreign intelligence purposes be only allowed if strictly necessary. (p. 34)
   g) That "publicly available information" be limited to commercially available publications and broadcasts, and its collection only be approved by the Intelligence Commissioner if strictly necessary for CSIS to carry out its mandate. (p. 34)
3. That CSIS agents, and individuals at their direction, not be granted immunity for "acts or omissions that would otherwise constitute offences". (pp. 34-35)

Part 5: ***Security of Canada Information Disclosure Act*** (p. 37)

1. SCISA should be rescinded and be replaced by strong privacy protections regulating the sharing of information for national security purposes. (p.38)
2. Barring this, we recommend that the definition activity that undermines the security of Canada in section 2 be replaced with the following:
   activity that undermines the security of Canada means any activity that threatens the lives or the security of people in Canada or of any individual who has a connection to Canada and who is outside Canada. For greater certainty, it includes
   (a) interference with the capability of the Government of Canada in relation to defense or public safety;
   (b) changing or unduly influencing a government in Canada by force or criminal means;
   (c) espionage, sabotage or covert foreign-influenced activities;
   (d) terrorism;
   (e) proliferation of nuclear, chemical, radiological or biological weapons;
   (f) significant or widespread interference with the global information infrastructure;
   (g) conduct that takes place in Canada and that threatens the lives or security of people in another state. (p. 38)
3. That section 2(1) be replaced with, "For the purposes of this Act, advocacy, protest, dissent or artistic expression is not an activity that undermines the security of Canada unless carried on in conjunction with an activity intended to cause death or bodily harm, endanger life, or cause serious risk to health or public safety." (p. 38)

4. That an exception also be included to cover actions relating to Indigenous sovereignty, land claims, or title rights. (p. 38)

Part 6: *Secure Air Travel Act* (p. 39)

1. That the Safe Air Travel Act should be repealed and the Passenger Protect Program be ended. (p. 41)
2. That, barring this:
   a) The government include clear guidelines for the creation of a redress system for false positives.
   b) Decisions to add an individual to the list should be reviewed and approved by a court.
   c) Individuals should be given written notice that they have been listed.
   d) That in defending their listing, an individual and their counsel, have full access to the information and evidence being presented in support of the listing. (p. 41)

Part 7: Amendments to the *Criminal Code* (p. 42)

1. That the superfluous and repetitive offence of "counselling terrorism offenses" be removed. (p. 42)
2. That, similar to the changes to preventative detention, the threshold for peace bonds should be increased to "necessary" to prevent a crime. (p. 42)
3. That Bill C-59 should repeal the "Terrorist Entities Listing" in favour of simply using laws that already prohibit organizations from taking part in criminal activities. (p. 42)

Parts 8 & 9: *Youth Criminal Justice Act* & Review (p. 43)

1. That the review period be reduced to five years for new oversight and review mechanisms and to three years for new CSIS and CSE powers. (p. 43)

What's missing from Bill C-59 (p. 44)

1. That a strong review mechanism to look at CBSA and its activities outside of national security be created. (p. 44)
2. That provisions that put an end to the security certificate regime be added. (p. 44)
3. That a provision outlawing the use of TUSCAN by Canadian border agents be included. (p. 45)
4. That a provision outlawing the use of the US No-Fly List by airlines in Canada for flights that are not going to and/or through the US be added. (p. 45)

Part 1: The *National Security and Intelligence Review Agency Act*

The creation of a National Security and Intelligence Review Agency (NSIRA or Agency) with an ability to review all government activities related to national security is a very welcome development. The ICLMG has long supported the creation of such an overarching body, and believe it will have a significant, positive impact on transparency, accountability and effectiveness of Canada's national security activities.

We also believe that this presents an important opportunity to learn from concerns that have been expressed regarding existing review agencies. By ensuring that these issues are not transferred to the new agency, the government can ensure that the NSIRA starts off on the right footing.

1. Composition of the NSIRA

We believe that the minimum of three members (plus the Chair) is too low for the NSIRA to effectively carry out its work, and would also hinder the diversity of opinions, expertise and backgrounds of Agency members. We recommend that the minimum number be set at five and the maximum number be increased to eight (in addition to the Chair).

Second, we believe that it is important that members of the Agency have the utmost independence from the government. While section 4(2) mandates consultation with opposition parties in deciding membership, we believe a stronger mechanism is necessary. We would propose that instead, nominations be carried out in consultation with opposition parties, and that the final appointment be made by a vote in the House of Commons, requiring a 2/3 majority.

We would also encourage the government, in considering nominations to the NSIRA, to look to creating a membership with not only a background in national security, but also includes people from diverse communities and multiple sectors – including those with an expertise in civil liberties and human rights. This would help ensure effective and in-depth recommendations and reports.

2. Complaint process

The proposal of integrating the complaints process for the Canadian Security Intelligence Service (CSIS), Communications Security Establishment **(**CSE) and Royal Canadian Mounted Police (RCMP) national security activities into one review agency is a positive development. However, we believe that there should be a process for individuals to submit complaints on more than just these three agencies, especially since the government considers at least 17 agencies and departments to be involved in national security-related operations (we have been unable to get the exact number).

The most glaring absence is the Canadian Border Services Agency (CBSA). The CBSA has a clear national security mandate and often takes action based on national security

prerogatives. While NSIRA will have the power to study CBSA's activities, individuals should also have the power to file complaints with an independent body regarding CBSA's national security activities.

Global Affairs Canada – particularly through consular affairs – also plays a key role in national security. This is especially true regarding Canadians detained or surveilled abroad. Indeed, Canadian diplomatic and consular officers have played key roles in the mistreatment and torture of individuals such as Maher Arar, Abdullah Almalki, Ahmad El Maati and Muayyed Nureddin, all detained and tortured abroad. By including Global Affairs Canada in this complaints mechanism, we would have greater certainty around accountability and review for when Canadians' rights are not respected abroad.

We therefore recommend that the complaints mechanism be amended to apply to all federal national security activities, regardless of department. At a minimum, it should be modified to include both CBSA's and Global Affairs Canada's national security activities.

3. Department studies

The ability for the NSIRA to "review any activity carried out by a department that relates to national security or intelligence" as well as the power to "direct [a] department to conduct a study" of its national security related activities is again a welcome addition.

However, we would urge more clarity on these departmental studies and the overall review process. We recommend adding a more specific requirement under "Public Reports" that would mandate a listing of each departmental study requested, and its result. This would ensure transparency around the review process, particularly for departments not subject to the NSIRA complaints mechanism.

4. Recommendations of the NSIRA

As mentioned earlier, we believe that the creation of the NSIRA grants an opportunity to address concerns with existing independent review bodies. These concerns include the inability of the bodies to make binding recommendations, as well as a lack of transparency around implementation and follow-up. This has been a particular issue regarding the Security and Intelligence Review Committee (SIRC), CSIS' current review body. A lack of clarity in public reports often make it difficult to ascertain what recommendations are being made, what aspects are or are not being implemented, and whether they have been effective in addressing the root of the complaint. It is understandable that some vagueness is necessary for operational reasons. By allowing SIRC to make binding recommendations, though, we could be more certain that the issues identified are being fully resolved.

It is understandable that there is concern around an unelected, appointed body making binding recommendations for a national security agency. However, if we consider that the NSIRA plays — or, as we believe, should play — a similar role to a Commissioner of

Inquiry, it is reasonable for it to have order-making powers. We therefore recommend that the Agency be granted binding powers to enforce specific actions by the national security agencies.

Finally, follow-up and results of the review agency's recommendations should be made more transparent. This could be achieved by mandating, in the legislation regarding public reports, a clear section containing a listing of previous recommendations, and actions taken to address them.

5. Transparency

According to the Investigations section of the NSIRA Act, "every investigation by the Review Agency is to be conducted in private" [25(1)], "no one is entitled as of right to be present during, to have access to or comment on representations made to the Agency by any other person" [25(2)], and that, while the Agency "must report the findings of the investigation to the complainant," it is only held to the threshold of "**may** report to the complainant any recommendation it sees fit."

These articles are similar to those currently in place for SIRC, which have led to serious concerns regarding transparency of investigations, findings and recommendations.

First, regarding 25(2), it is troubling that a complainant is not guaranteed access to all information presented during a complaints process, especially in order to respond to rebuttals of their complaint. We believe that complainants should have access to all information necessary in order to support their complaint, and to respond to information presented to the Agency or others.

Second, under the proposed legislation, the disclosure of recommendations to the complainant is left to the discretion of the Agency. We would argue that the complainant has a right to know all recommendations made by the Agency in order to ensure that their complaint is being properly resolved. Therefore, we recommend adding a clause that obliges the Agency to disclose all recommendations resulting from a complaint to the complainant.

Finally, the clause that all hearings are held in private must be clarified. This issue is highlighted by the current lawsuit filed by the British Columbia Civil Liberties Association (BCCLA) against SIRC about a complaint made by environmental organizations regarding CSIS surveillance activities.[2] Based on the understanding that investigations take place in private, the complainants have been told by SIRC they are not allowed to publicly disclose any aspects of the proceedings – including the written submissions filed by the complainants.

---

[2] Platt, Brian. "Civil liberties group takes Canada's spy watchdog to court over monitoring of pipeline protesters," *National Post*, Oct. 4, 2017. Online: https://nationalpost.com/news/politics/civil-liberties-group-takes-canadas-spy-watchdog-to-court-over-monitoring-of-pipeline-protesters

If independent review agencies are to be effective in holding national security agencies to account, it is imperative that their work be carried out in as public a manner as possible. This is not only to ensure the accountability of the security agencies in question, but also to maintain the credibility of the review process itself.

We therefore recommend that the committee amend these sections to ensure transparency and accountability of the review and reporting process itself, and that all representations and recommendations be made available to complainants.

6. Redress

A very problematic feature of SIRC, CSIS' current watchdog, is its complete lack of redress even if the committee finds that an abuse was committed. The proposed legislation to create the NSIRA does not fix this problem. For example, neither current SIRC legislation nor proposed NSIRA rules provide for compensation or reimbursement of legal fees, again, even if abuse was found. In order for this review mechanism to be truly accessible and to repair the damage done by the national security agencies — and increase their accountability — the NSIRA should be able to rule on and offer redress to complainants.

Recommendations:

1. a) That the minimum number of members of the NSIRA be set at 5 and the maximum number be increased to 8 (in addition to the Chair).
   b) That, in addition to nomination of NSIRA members being carried out in consultation with opposition parties, the final appointment be made by a 2/3 vote in the House of Commons.
   c) That the membership will include people from diverse communities and multiple sectors – including those with an expertise in civil liberties and human rights.
2. That the NSIRA complaints mechanism be amended to apply to all national security activities, regardless of department. At a minimum, it should be modified to include both CBSA's and Global Affairs Canada's national security activities.
3. That a more specific requirement be added under "Public Reports" to mandate a listing of each departmental study requested, and its result.
4. a) That the NSIRA be granted binding recommendation powers.
   b) That the NSIRA's annual public reports include a mandatory follow-up and review of previous recommendations.
5. That the complaints investigation and reporting mechanisms be amended to ensure greater transparency and accountability; that complainants get access to all the information necessary to their case; that all representations or recommendations made during the complaints investigation process are available to complainants; and that, to the greatest degree possible, complaint findings are released to the public.
6. The NSIRA should be able to rule on and offer redress to complainants.

Part 1.1: The *Avoiding Complicity in Mistreatment by Foreign Entities Act*

During study of Bill C-59 at the House of Commons Standing Committee on Public Safety and National Security, Liberal members introduced the *Avoiding Complicity in Mistreatment by Foreign Entities Act*.

Liberal MPs described the act as enshrining in law rules that would prevent Canadian agencies from using information tied to regimes that engage in torture or mistreatment, and prevent Canadian agencies from sharing information that would lead to mistreatment or torture. Unfortunately, the new Act falls far short.

The Act does take the important step of mandating that all major departments and agencies involved in national security must have a ministerial direction regarding "avoiding complicity in mistreatment by foreign entities," that such ministerial directions must be made public, and that the agencies make annual reports to the appropriate minister on their adherence to these directions, as well as to the National Security and Intelligence Committee of Parliamentarians and any relevant review body. A vetted version will be tabled in Parliament and made public (more details on this below).

This is a change from the current system where no such ministerial directions are mandatory, and where any such directions are by default secret until the government decides otherwise.

However, outside of the preamble, the new Act does not establish what these guidelines must include. In Fall 2017, the Liberal government released revised ministerial directions regarding avoiding complicity is mistreatment by foreign entities. While an improvement on previous ministerial directions, these new regulations remained lacking in several areas. Most concerning is that they still allow, under certain circumstances, for Canadian agencies to use information obtained through mistreatment or torture; a completely unacceptable stance.[3]

There is also nothing in the Act that would prevent this or any future government from further weakening ministerial directions, as we have seen in the past. The argument that the public nature of the directives will lead to a political cost for future governments that seek to weaken the rules is unconvincing. We have already seen that changes to such directives often elicit little public scrutiny, and that when there is criticism, it is rebuffed under the argument of "national security concerns." The protection of rights must be enshrined, and not simply left to be guarded by public pressure.

---

[3] See: ICLMG, "New Ministerial Direction Falls Short On Fulfilling Goal Of Preventing The Sharing, Requesting Or Use Of Information Tied To Torture." September 25, 2017. Online: http://iclmg.ca/newministerial-direction-on-avoiding-complicity-in-mistreatment-by-foreign-entities-falls-short-on-fulfillinggoal-of-preventing-the-sharing-requesting-or-use-of-information-tied-to-torture/

While the addition of new reporting requirements is also welcome, they also do not go far enough. This is particularly true regarding the reports filed with Parliament and made public. Before being released, reports will be vetted for information "which would be injurious to national security, national defence or international relations or compromise an ongoing operation or investigation" and for information covered by solicitor-client privilege. These exclusions – particularly information related to the vague term "international relations" – are much too broad and raise concerns that there will be an important public accountability gap.

Recommendations:

1. That this new Act be replaced with clear guidelines outlawing, in all circumstances, the use or sharing of information that will make Canada and its government agencies complicit in foreign mistreatment or torture, and that yearly reporting by departments on how they fulfilled this obligation be made mandatory.
2. That annual reports on adherence to directions on avoiding complicity in mistreatment by foreign entities not be subject to undue vetting. To that end, the provision allowing for their redaction based on injury to "international relations" should be removed.

Part 2: The *Intelligence Commissioner Act*

Much like the NSIRA, we welcome the proposal of a new Intelligence Commissioner (IC or Commissioner) and the important oversight role the Commissioner will play in approving ministerial authorizations before surveillance activities take place.

However, much like the NSIRA, we believe there are ways the *Intelligence Commissioner Act* could be improved.

1. Appointment and term of the Commissioner

It is important that the IC be completely independent of the government. Therefore, we recommend that the Commissioner be nominated by the Governor in Council, but be approved by a 2/3 vote in the House of Commons.

Further, we believe that given the important role the Commissioner will play, they should be appointed on a full-time, rather than a part-time basis.

Finally, we would recommend that the IC not be restricted to being a retired superior court judge, and that the pool for selection should also include active superior court judges.

2. Reporting

In the first version of Bill C-59, we noted an important missing piece: the lack of a requirement for the Intelligence Commissioner to issue a public report. We are therefore pleased that in the current version of the Bill, this has been added in part 22 (1) to (3).

In our original brief, we also raised concerns that, while the IC would be required to provide their written decisions to the NSIRA, the Commissioner would not be required to set out their reasons for approving an authorization. This too has been changed in the latest version of the Bill, in 20 (1)(a).

We remain concerned, though, that while the IC must provide their decisions to the NSIRA, nothing in the *NSIRA Act* details what the Agency must do with these decisions.

We would therefore recommend that the NSIRA be mandated to include a section regarding the work of the Intelligence Commissioner in its reporting, including an external review of their work.

It is important that such a crucial oversight entity be accountable and transparent to ensure its effectiveness and credibility. We need only to look to the Foreign Intelligence Surveillance (FISA) courts in the United States for an example, where secrecy, lack of transparency and lack of accountability eroded the courts' ability to effectively oversee the NSA's activities. It is imperative that we learn from this experience and ensure that there is more transparency in the Canadian system.

3. Powers

As explained further in the section on the Communications Security Establishment, the Intelligence Commissioner should be required to play a larger role. The IC should be able to impose conditions on approved authorizations, and their approval should be necessary in addition to the consent of the Minister of Foreign Affairs for all defensive cyber authorizations. If there are to be any active cyber authorizations, we believe more rigorous oversight is required. This is discussed further in the section on the *CSE Act*.

Recommendations:

1. a) That the IC be nominated by the Governor in Council, but approved by a 2/3 vote in the House of Commons.
   b) That the IC be appointed on a full-time, rather than a part-time basis.
   c) That the pool for selection should also include active superior court judges.
2. That the NSIRA be mandated to include a section regarding the work of the IC, including an external review of their work.
3. a) That the IC be able to impose conditions on approved authorizations.
   b) That both the approval of the IC and consent of the Minister of Foreign Affairs be required for all cyber operation authorizations.

Part 3: The *Communications Security Establishment Act*

The ICLMG would like to highlight the importance of finally legislating the Communications Security Establishment (CSE), considering it has been active since World War II, under one form or another. However, we would also note that legislating CSE's powers should not just be accepted based on the fact the agency has been carrying out this work for more than 70 years. The federal government must demonstrate to the public that these existing powers — in addition to the new powers introduced by Bill C-59 — are necessary to keep Canadians safe and that they respect the *Charter of Rights and Freedoms*. This is especially true when it comes to the CSE's ability to engage in "activities that would otherwise constitute offences" (CSE Act, s. 3).

1. Mandate

The CSE's mandate is expanded under Bill C-59, to now include active and defensive cyber powers. While the scope remains the same for much of its activities, the "active cyber operations" mandate of the CSE covers defence, security and international affairs. We do not believe that "active" cyber operations can be justified for defence or security reasons – especially when potential retaliation for such cyber attacks could endanger our security (more details in section 14). We also strongly disagree that "international affairs" is a sufficient reason to launch cyber operations.

Instead, the CSE's mandate should continue to be limited to defence and national security, and thus active cyber operations should not be added. In any case, "international affairs" should be removed from the CSE's mandate.

2. Activities directed at Canadians

The Canadian government and the CSE have repeated for years that the CSE's activities are not directed at Canadians or people in Canada, which is prohibited under their mandate. However, the establishment's record shows this is untrue.

First, while the CSE's overall mandate is "foreign facing," one category of the CSE's activities is not restricted from being "directed at Canadians": technical and operational assistance. This category of activities continues to be very vague and broad, allowing the CSE to assist other agencies in unknown ways in spying on Canadians.

Second, in 2012, the CSE was shown to be spying on Canadians using airport wi-fi networks, tracking their movements. The agency — and its watchdog — claimed this was a "test" and within their mandate, since they only collected metadata. But as several digital and privacy experts have pointed out, metadata can reveal important amounts of private information about a person: where they have been, who they talk to, what they believe in, etc.

Bill C-59 will also grant the CSE new information gathering powers, including the ability to collect "publicly available information." Canadians or people in Canada will not be

excluded from this new power, meaning that so long as information is publicly available, the CSE will be able to collect it.

This is on top of the fact that the CSE had, in 2013, failed to anonymize Canadians' metadata that it collected while conducting foreign surveillance, and subsequently shared with international partners. It is unclear how long the CSE was aware of the issue before reporting it either to government or to the CSE Commissioner, but the details were only revealed publicly in 2015.

Finally, the CSE is also supposedly restricted in its mandate regarding Active and Defensive cyber-operations to not target a part of the global information infrastructure that is Canadian. However, the inter-connectedness of this structure means that attacking one part of the system would very likely impact Canadians and people in Canada.

We therefore recommend that greater restrictions be placed on any CSE actions directed at Canadians or people in Canada. In particular, we believe that a warrant should be required for any activities that could implicate Canadians or people in Canada, including activities related to the CSE's technical and operational assistance to other law enforcement and intelligence agencies such as the RCMP and CSIS. This is particularly important in the context of CSIS's new disruption powers introduced by Bill C-51 (the *Anti-terrorism Act of 2015*).

Overall, more must be done to ensure that the CSE's activities cannot target Canadians or people in Canada. This could include both increasing the powers of the Intelligence Commissioner to review all of the CSE's activities, as well as narrowing the scope of surveillance and cyber activities.

3. Metadata

There are also other, extenuating issues regarding metadata. As mentioned above, metadata is often dismissed as not being private information under the incorrect pretense that it does not reveal personal details.

It is unclear if this is why a loophole regarding metadata exists in the bill. However, according to s. 23 of the new *CSE Act*, the CSE must acquire an authorization for any act of collection that would contravene an Act of Parliament. However, not all privacy-protected information would fall under this category – including metadata.

Metadata would therefore not be considered off-limit, allowing the CSE to sweep up Canadians' private information. The result would essentially legalize mass surveillance.

The *CSE Act* should define metadata, strongly limit its collection, use and retention, and require a warrant to collect it.

4. Ministerial authorizations

The CSE Act stipulates that Ministerial authorizations are needed when the establishment's actions regarding surveillance and cyber security will contravene other acts of Parliament, meaning breaking the law. While these authorizations will need to be approved by the Intelligence Commissioner, we believe that, as it is currently structured, this is insufficient. Our concern is that approvals such as this, conducted in secret, can and have resulted in secret legal analysis, untested outside of the national security sphere. Further, we need only look to the United States for a cautionary tale: similar mechanisms there — such as the FISA court — have a track record of rubber-stamping warrants, becoming more and more permissive over time, and allowing for surveillance to be deployed on massive scales, violating the rights of millions of Americans. The only reason we know this is because of the work of Edward Snowden. A similar system in Canada could very well have similar results.

The *CSE Act* also allows Ministerial authorizations in order to gain access to a portion of the global information infrastructure (GII). While the GII is defined in the new *CSE Act*, it is still unclear what it would mean in concrete terms. We believe this is too vague and broad. Could it mean access to an entire underwater optic cable? If that is the case, it's too much. Collection should always be narrowly targeted.

We are further concerned by the ability for Ministerial authorizations to allow for the collection of "unselected" information. In essence, unselected information is not tied to any selector (ie, criteria or keyword) and is thus a clear form of mass surveillance, in violation of both international human rights and Charter protected privacy rights.[4] While authorizations are meant to allow activities that are "reasonable and proportionate," we would argue that such activities can never be considered proportionate to a particular security concern. We would suggest that the targeting of unselected information be removed from the *CSE Act*, or, at a minimum, that the Intelligence Commissioner be granted the powers to rule that such actions are disproportionate, and/or impose binding limits.

The Act also stipulates that the foreign surveillance collected through Ministerial authorizations should not be retained for longer than is reasonably necessary. "Reasonably" is vague and arbitrary. The information collected should not be retained longer than *necessary* to fulfill the intended objective. Analysis of the information should be swift to ensure that the unnecessary information is destroyed expediently.

[4] Report of the Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age", Advanced Edited Version, June 30, 2014, A/HRC/27/37, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; Tamir Israel. (2015). "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation." in Michael Geist (Ed.). Law, Privacy and Surveillance in Canada in the Post-Snowden Era. Ottawa: University of Ottawa Press, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

We also find it problematic that there does not seem to be a retention limit on information collected for cyber security purposes. We would therefore suggest a similar limitation, that the information be retained only so long as it is necessary. If technical information collected is needed for ongoing work, the CSE should be able to make a case for longer-term retention. An indefinite retention period without restrictions, however, would be unwarranted.

Ministerial authorizations last one year, and up to two years with an extension. Extensions are not subject to review by the Intelligence Commissioner. Also, the Intelligence Commissioner is only notified of changes to authorizations if the Minister believes it is "significant." First, one year is too long to spy on anyone or any portion of the information infrastructure without periodic reviews to ascertain that the collection is still necessary. Second, the extension and changes should also not be done without the examination and approval of the Intelligence Commissioner.

It is difficult to suggest specific recommendations regarding the CSE's authorizations without addressing the fundamental concerns raised by surveillance authorized in secret. For example, while we welcome the introduction of the Intelligence Commissioner role, and suggest in this brief ideas for improvements to strengthen this office, it is still difficult to fully accept that, without greater independence and transparency, there will be sufficiently strong oversight to reduce the overreach we have seen in the past as well as strict controls over the newly expanded CSE powers found in Bill C-59.

We therefore find that the committee should examine a dual approach: increasing the independence and transparency of the work of the Intelligence Commissioner and, to the greatest amount possible, ensure that the CSE's powers and authorizations are narrowly defined. Doing so will aid both in reducing potential overreach from the beginning, and ensure that there is strong oversight and reporting as a secondary measure.

It is also imperative that the Canadian government continue to question, in a fundamental manner, and to provide evidence to the public as necessary, as to the effectiveness and necessity of surveillance – especially if it is approved in secret. We also suggest that under no circumstances should the Canadian government – including the CSE – engage in the type of mass surveillance that, unfortunately, it appears has already become a norm, both in Canada and internationally.

5. Publicly available information

The *CSE Act* stipulates that the CSE "can acquire, use, analyse, retain or disclose publicly available information." Once again, this is too vague and broad and we believe will allow the unnecessary collection of troves of information that could lead to the creation of

profiles on thousands and thousands of Canadians, as the Privacy Commissioner of Canada has already warned.[5]

It has also been pointed out that the wording would allow the CSE to acquire this publicly available information via various means. For example, leaked information from a hack becomes "publicly available information." Buying information from data brokers — with our tax dollars — thus encouraging an industry based on syphoning up private information, would also not be excluded under the Act.

The CSE has argued that this provision would simply allow the collection of public reports and information that is necessary to their work, but unrelated to their mandate. If that is true, it should be specified as such. Otherwise, any collection of public information should be subject to narrow restrictions, approved by the Intelligence Commissioner, and subject to similar safeguards as those for other CSE information collection practices.

We would therefore support the proposal put forward by Citizen Lab and CIPPIC in their joint report on the CSE that:

- "Publicly Available Information" be limited in application to commercially available publications and broadcasts.
- Paragraph 23(1)(a) of the *CSE Act* be amended so that the CSE may only acquire, use, analyze and retain information despite the restrictions in sub-sections 22(1) and (2) if such information falls within a dataset that the Intelligence Commissioner has approved as necessary to the foreign intelligence or cybersecurity and information assurance aspects of the CSE's mandate.[6]

6. Investment Canada Act

Subsection 24(2) of the *CSE Act* creates an exception to the rule that the CSE cannot target Canadians or people in Canada in its activities in relation to the *Investment Canada Act*. While this may be a necessary provision in order to review sensitive business operations in Canada, the committee should impose greater restrictions, including limits on how information is collected, retained, analyzed and disposed of.

---

[5] Sources: http://nationalpost.com/pmn/news-pmn/canada-news-pmn/security-bill-needs-safeguards-to-prevent-a-profile-on-all-of-us-privacy-czar; https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2017/parl_20171207/

[6] See: Parsons, Christopher A. and Gill, Lex and Israel, Tamir and Robinson, Bill and Deibert, Ronald J., Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (an Act Respecting National Security Matters), First Reading (December 18, 2017), p. 54. Transparency and Accountability, December 2017. Available at SSRN: https://ssrn.com/abstract=3101557 or http://dx.doi.org/10.2139/ssrn.3101557

7. Information acquired incidentally

In its operations, the CSE does and will continue to collect Canadian information incidental to its foreign surveillance activities (s. 24(4)). While this may be unavoidable, the government should make it clear to the public that their information could be swept up if they are communicating with people abroad who are targeted by CSE's activities. Again, the CSE needs to be more honest publicly about how they carry out their surveillance and what information they collect in Canada/from Canadians. And more importantly, beyond restrictions on how information is collected, a strict limit on how long this incidentally acquired information can be retained should be added to the *CSE Act*. Currently, this is left to the Minister's discretion when issuing authorizations (s. 36); it should instead be prescribed in the Act that such information can only be retained so long as it is necessary for protecting the security of people in Canada.

8. Privacy protections

Section 25 of the *CSE Act* stipulates that the CSE must ensure that measures are in place to protect Canadians' privacy when information about them is incidentally collected and the information is publicly available. However, it fails to mention what those privacy protections are and how they will be determined. This is a very important oversight, as the CSE has tremendous capabilities to violate privacy rights.

Furthermore, privacy protections in place before Bill C-59 was introduced did not stop the agency from carrying out activities, revealed by Edward Snowden and the media, that clearly disregarded the privacy rights of Canadians, as well as non-Canadians, in Canada and abroad. To name a few problematic actions, the CSE:

- Allowed the NSA to create a "backdoor" in an encryption key used worldwide;
- Captured millions of downloads daily;
- Engaged in mass surveillance of file-sharing sites;
- Developed cyber-warfare tools to hack into computers and phones all over the world;
- Shared information on Canadians with its foreign partners without proper measures to protect privacy (and the data was later erased from the agency's system making it difficult to find out the number of people impacted by the privacy breach).[7]

How can we trust that this time around the privacy protections will be enough? These protections should not be determined by the agency that does the data collection, and they should not be secret either. The *CSE Act* must enshrine in law strong privacy protections around CSE's activities. The culture of the agency also needs to change, the problematic

[7] Sources: http://liguedesdroits.ca/?p=2118; https://theintercept.com/2015/01/28/canada-cse-levitation-mass-surveillance/; http://www.thestar.com/news/canada/2015/04/01/canadas-spy-review-bodies-struggling-to-keep-tabs-on-agencies.html; http://www.cbc.ca/news/politics/spy-canada-electronic-metadata-1.3423565; http://www.thestar.com/news/canada/2016/01/29/a-privacy-breach-and-a-country-left-in-the-dark-tim-harper.html; http://www.cbc.ca/news/politics/cse-metadata-five-eyes-sharing-1.3459717?cmp=rss.

actions, including those revealed by Edward Snowden, need to be outlawed, and stronger safeguards than the ones currently proposed by C-59 need to be implemented.

9. Protection of infrastructure

Section 28(1) of the *CSE Act* on the protection of federal and non-federal infrastructure should include provisions against use or disclosure of the acquired information for any other purpose than to protect the information infrastructure from mischief, unauthorized use or disruption.

10. Disclosure of Canadian identifying information

Section 44 of the *CSE Act* states that Canadian identifying information can be disclosed to a designated person only if the CSE "concludes that the disclosure is essential to international affairs, defence, security or cyber security." While “essential” is a strong threshold, we believe that there should be outside review to ensure the proper adherence to both the disclosure threshold and who is appointed a designated person. We suggest adding a provision wherein the minister must report to either the Intelligence Commissioner or Privacy Commissioner who has been designated, and the reasoning for any disclosure. The reviewing body should be granted powers to make binding rulings should they see fit. Reports should also be shared with the NSIRA.

Furthermore, in 2016, it was revealed that in 2013 the CSE discovered it was sending information on Canadians to our Five Eyes allies without proper scrubbing to hide identities. How many Canadians? We don’t know. It was also revealed that the Conservative government in power at the time knew about the breach and decided to hide it from the Canadian public. It is unclear how C-59 would protect us from such a lack of candour in the future. However, it can be minimized by increasing the reporting requirements and ensuring robust powers for the Intelligence Commissioner.

11. Arrangements

Section 55 of the *CSE Act* allows for arrangements to share information or cooperate with foreign agencies and states. These arrangements are a potentially very dangerous practice that can lead to human rights violations and torture, like in the cases of Maher Arar, Abdullah Almalki, Ahmad Elmaati and Muayyed Nureddin.

They should be strongly regulated, limited and approved by the Intelligence Commissioner, not just the Minister. It should be necessary for the Intelligence Commissioner to explicitly determine the likelihood that bodily harm – including mistreatment or torture – could be at play in any arrangement. We would also recommend that the Intelligence Commissioner integrate such an analysis into all Ministerial authorization approvals.

12. Confidentiality

Section 56(5) of the *CSE Act* states that judges must ensure the confidentiality "(a) of the identity of any person or entity that has assisted or is assisting the CSE on a confidential basis; and (b) of information if, in the judge's opinion, its disclosure would be injurious to international relations, national defence or national security or would endanger the safety of any person."

This confidentiality principle is very broad and we are concerned that it could hinder due process. Safety of a person is a *Charter* right, and has the same importance as the right to due process, therefore it can be argued in court which right should have priority on a case by case basis. International relations, defence and national security should not be used to hinder due process — as it so often is.

Section 56(5) should include an exception preventing the judge from ordering that confidentiality be respected if it hinders due process.

13. Five Eyes

The CSE is part of what is known as the Five Eyes, an alliance of spy agencies from the US, the UK, New Zealand, Australia and Canada. Officially, these countries do not spy on each other, but it has long been established that the Five Eyes do spy on their allies, and that they exchange information on each other's citizens[8]. This practice is not addressed in the *CSE Act*.

We recommend that this practice of using intelligence garnered by allies to skirt domestic surveillance regulations, particularly when it comes to the Five Eyes, be outlawed in the legislation.

14. New cyber operation powers

The *CSE Act* also grants the national security agency new and very concerning defensive and active cyber operation powers. According to the bill, cyber powers could include "installing, maintaining, copying, distributing, searching, modifying, disrupting, deleting or intercepting anything on or through the global information infrastructure" and "carrying out any other activity that is reasonable in the circumstances and reasonably necessary in aid of any other activity, or class of activities, authorized by the authorization." This is too broad and should be narrowed to only allowing activities that are strictly necessary to protect the security of people in Canada.

Furthermore, a report on cyber activities will be shared with the new National Security and Intelligence Review Agency (NSIRA), but with no guarantees that there will be any public reporting. These powers are akin to military actions, which could cause retaliation,

[8] http://www.michaelgeist.ca/2013/11/csec-spying-csis/

and should be discussed publicly. Greater restrictions should also be placed on them, including oversight and reporting from the Intelligence Commissioner.

On November 12, 2017, the *New York Times* reported that there had been a major leak of NSA cyberweapons, which were in turn used to hack businesses and civilians worldwide.[9] Offensive hacking can therefore not only make us unsafe because of potential retaliation, these cyberweapons could be leaked, making us the targets of criminals.

Therefore, we support the British Columbia Civil Liberties Association's position on 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."[10] Therefore, the ICLMG recommends that:

- Cyber threats not be used to expand domestic surveillance powers
- The creation and use of any cyberweapons be strongly limited;
- Cyber security initiatives have genuine oversight and be more transparent;
- Cyber operations only allow defensive purposes, not active/offensive cyberattacks.

Barring the outlawing of active cyber operations, one specific issue in Bill C-59 can be addressed right away. The power to carry out an "active" cyber operation can be triggered solely through a decision by the Minister of National Defense, in consultation with the Minister of Foreign Affairs. While the Act sets out certain restrictions, we believe these are insufficient. The approval of the Intelligence Commissioner or of Parliament should be required.

General recommendations

A. That the Intelligence Commissioner be empowered to review all of CSE activities.
B. That the government take steps to further narrow the scope of the CSE's surveillance and cyber activities overall.
C. That, to ensure accountability of the CSE, the independence and transparency of the work of the Intelligence Commissioner be strengthened and, to the greatest amount possible, the CSE's powers and authorizations be narrowly defined.

Specific recommendations

1. That "international affairs" be removed from the Communications Security Establishment's (CSE) cyber operations mandate.

---

[9] https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

[10] https://bccla.org/wp-content/uploads/2018/02/2017-01-30-Written-Submissions-of-the-BCCLA-to-SECU_Bill-C-59.pdf; see also https://citizenlab.ca/wp-content/uploads/2017/12/C-59-Analysis-1.0.pdf pp 31-32.

2. That more must be done to ensure that the CSE's activities actually cannot target or implicate Canadians or people in Canada. In particular, a warrant should be required for any activities that could implicate Canadians or people in Canada, including activities related to the CSE's technical and operational assistance to other law enforcement and intelligence agencies such as the RCMP and CSIS.
3. That the *CSE Act* should define metadata; strongly limit its collection, use and retention; and require a warrant for metadata collection.
4. a) That Ministerial Authorizations of surveillance operations be restricted to a precise and narrow target.
   b) That the targeting of unselected information be removed from the *CSE Act,* or, at a minimum, that the Intelligence Commissioner be granted the powers to rule on whether such actions are disproportionate, and/or impose binding limits.
   c) That information collected should not be retained longer than *necessary* to fulfill the intended objective.
   d) That Ministerial Authorizations be reduced to the amount of time *necessary* to fulfill the intended objective, and any extension and changes should only be done with the examination and approval of the Intelligence Commissioner.
   e) That the Canadian government not engage in mass surveillance. Barring that, that it at a minimum questions the use of mass surveillance, and provides evidence to the public as to the effectiveness and necessity of surveillance – especially if it is approved in secret.
5. a) That the definition of "publicly available information" be limited in application to commercially available publications and broadcast, that further restrictions be placed on any collection of such data.
   b) That the CSE may only acquire, use, analyze and retain publicly available information if such information falls within a dataset approved by the Intelligence Commissioner.
6. That greater restrictions be imposed on the CSE's carrying out of work in support of the *Investment Canada Act,* including limits on how information is collected, retained, analyzed and disposed of.
7. That incidentally acquired information can only be retained so long as it is necessary for protecting the security of people in Canada.
8. a) The *CSE Act* must enshrine strong privacy protections around CSE's activities into law.
   b) The problematic actions of the CSE, including those revealed by Edward Snowden, need to be outlawed.
9. That information gathered in order to protect information infrastructure from mischief, unauthorized use or disruption not be disclosed for any other purpose.
10. That, regarding designating persons for the purpose of disclosure of Canadian identifying information, the Minister of Public Safety should report such a designation and the reasons for the disclosure to either the Intelligence Commissioner or Privacy Commissioner, who may then rule on it. These reports should also be provided to the NSIRA.
11. a) That all arrangements with foreign countries be strongly regulated, limited and approved by the Intelligence Commissioner.
    b) That when sharing information with a foreign country, it is necessary for the

Intelligence Commissioner to explicitly determine the likelihood that bodily harm – including mistreatment or torture – could be at play in any arrangement.

c) That the Intelligence Commissioner include an analysis of what impact an authorization may have on mistreatment or torture in their written decisions.

12. That judges be prevented from ordering that confidentiality be respected if it hinders due process.

13. That the practice of the Five Eyes spying on each other, and the use of such information to skirt rules prohibiting the surveillance of Canadians or people in Canada, be outlawed.

14. a) That the definition of possible cyber operations be narrowed to only allowing activities that are strictly necessary to protect the security of people in Canada.

b) That cyber operation powers be considered akin to military actions and should be discussed publicly, and that further restrictions should be placed on them, including oversight and reporting from the Intelligence Commissioner.

c) That cyber threats not be used to expand domestic surveillance powers.

d) That the creation and use of any cyberweapons be strongly limited.

e) That cyber security initiatives have genuine oversight and be more transparent.

f) That cyber operations only allow defensive purposes, not offensive cyberattacks.

g) If active cyber operations are still allowed, that they require the approval of the Intelligence Commissioner or of Parliament.

Part 4: Amendments to the *CSIS Act*

Bill C-59 would bring several important changes to CSIS' operations, however we will focus on three specific areas:

1. Amendments to current threat reduction powers
2. The introduction of a system for CSIS to collect, retain and query specific datasets
3. Immunity for acts or omissions that would otherwise constitute an offence

1. CSIS threat reduction powers

The *Anti-Terrorism Act, 2015* (ATA) granted CSIS, for the first time, powers to not only collect information on threats to Canada's national security, but to take action to reduce these threats.

These threat reduction powers were some of the most controversial of the Act and lead to widespread critique, both of whether such powers (as worded) were compliant with the *Canadian Charter of Rights and Freedoms*, and whether these were powers that a spy agency should hold, regardless of constitutionality.

In our brief on the *ATA*, we wrote:

> Bill C-51 would amend the *CSIS Act* to confer extraordinary powers to Canadian security agents to violate the human rights of Canadians, all in secret. This extension of state power into private life, carried out largely in secret, is an invitation to abuse. Further, the system depends on the good faith and candour of CSIS, an agency that has a bad track record of "seriously misleading" courts and review bodies. The many cases of serious human rights violations by CSIS over the past 15 years heighten concerns that these "disruption" powers are unprecedented, dangerous, and have no place in a free and democratic society.[11]

Bill C-59 would bring changes in an attempt to limit these powers, to make them *Charter* compliant, and to increase after the fact review of CSIS' threat reduction activities.

Despite these proposed changes, our initial concerns remain and we continue to firmly oppose CSIS being granted these extraordinary powers. Bill C-59 does nothing to address the underlying problem of these threat reduction powers: that they grant powers similar to those of a law enforcement agency but without the transparency, accountability or adversarial nature of our criminal justice system.

By blurring the line between law enforcement and security intelligence, Bill C-59 continues to override the serious concerns that led to the creation of CSIS over 30 years

---

[11] Online at: http://iclmg.ca/wp-content/uploads/sites/37/2015/03/ICLMG-BRIEF-TO-THE-STANDING-COMMITTEE-C-51.pdf

ago. As we stated in 2015, it is imperative that we remember the lessons of the McDonald Commission, which concluded that security intelligence must be separated from law enforcement activities in order to protect our civil liberties. We therefore continue to hold that the threat reduction regime should be abandoned as an unsalvageable constitutional mess.

The central concern remains that if an organization is to conduct its work in secret, as CSIS does, its powers must be strictly controlled. Secrecy can both lead to abuse and overreach, but it can also inhibit the proper identification of mistakes, as well as limit the necessary rigor needed to ensure rights are protected.

Bill C-59 attempts to address these concerns in several ways, including:

- Wording re-iterating the primacy of the *Canadian Charter of Rights and Freedoms*;
- Creating an enumerated list of potential actions;
- Adding new limits to the scope of threat reduction powers (ie, cannot be used to detain an individual).

While these amendments would place greater limits on what threat reduction activities CSIS could engage in, they do not solve the underlying issue of law enforcement-type activities being authorized and carried out in secret. The concern is two-fold:

Authorization

Bill C-59 would continue the current situation of two kinds of threat reduction activities: those that require a warrant because of a potential limit on a *Charter* right, and those that do not require a warrant because no *Charter* right is implicated. This raises several concerns.

First, CSIS will determine whether a particular action meets the standard of limiting a *Charter* right. CSIS' past actions, though, raise questions about whether this standard can be decided in secret. As has been shown in court, for example regarding the retention of information by the Operational Data Analysis Centre, CSIS can and has in the past made their own secret legal interpretations that justify overreach. We should be concerned that CSIS, either through error or zeal, would be allowed to make decisions in secret about what actions do or do not limit a *Charter* right.

In those situations where CSIS does believe an action would violate a *Charter* right, they must seek warrant authorization from a judge. However, these judicial authorizations are made in secret, without the benefit of the adversarial process. Ensuring that warrants face some kind of adversarial process is a fundamental characteristic of our legal system, ensuring that the warrant was both justified and that government agents abided by the terms of the warrant. The current process does not – and, given the secrecy of CSIS' work, could never – integrate an adversarial process. Hence, such powers must remain with publicly accountable law enforcement agencies.

Finally, many observers raised concerns that requiring seeking judicial authorizations on a case-by-case basis to limit a *Charter* right is a significant departure in Canadian law, not comparable to search or surveillance warrants. Bill C-59 attempts to address that issue by creating a set list of actions that limit *Charter* rights and allowing a judge to decide whether a request falls under that list. We would argue that the result is still the same. However, even if it was seen as a judicially acceptable practice, the results would still be kept secret, running the risk of creating what Professors Forcese and Roach have described as a "secret jurisprudence." This result would continue to pose an important threat to Canadians' fundamental rights and freedoms.

Review

The proposed solution to this secrecy, in part, are rules requiring CSIS to report on its threat reduction activities to SIRC and, under C-59, an eventual National Security and Intelligence Review Agency (NSIRA). While on paper the new NSIRA would have broad powers of review, much of what they would investigate and eventually report back to government and to CSIS would remain secret. This is not a question of the integrity or work of those who serve as members of the Review Agency. It does mean, however, that the public, civil liberties advocates, and those people targeted by threat reduction activities, or even most parliamentarians, still do not have the power to examine, challenge or discuss these invasive powers.

Further, we are relying on CSIS being candid and straightforward with both the Review Agency and the courts. SIRC, in its 2016-17 report, reported that it believes CSIS up to this point has been following proper procedure in engaging in threat reduction activities. CSIS also reported to SIRC that it has not yet sought judicial authorization for any threat reduction activity. While on the surface this seems positive, the public is still unaware of the nature of CSIS threat reduction activities, which could still be very invasive even if not requiring a warrant. Further, as CSIS seeks out judicial authorizations, these activities will only become more sensitive. The fact that these powers have only recently been introduced also means the time period being examined is too narrow to give real clarity on how these powers will be used. At the same time, if we look to the past, there is a clear list of incidents that raise questions about whether review will be effective in reigning in these new, invasive powers.

We have seen that not only do review agencies not necessarily have access to all the information they need, but that CSIS has also deliberately misled or withheld crucial information. For example:

- In 2016, a Federal Court judge found that CSIS had illegally retained and analyzed data on people who posed no threat to national security. Moreover, the court found that CSIS failed to inform the court of these activities. And while the Security Intelligence Review Committee was informed of CSIS' activities, no

flags were raised, leading to questions about CSIS' transparency and SIRC's efficiency.[12]

- In its 2014-15 annual report, SIRC found that it had been "seriously misled" by CSIS and that CSIS agents had violated their duty of candour during ex parte proceedings.

- The Federal Court and Federal Court of Appeal both recently held that CSIS had breached its duty of candour and good faith to the Court and had obtained a warrant on the basis of evidence that was deliberately "crafted" to mislead and "keep the Court in the dark".[13]

- In the Almrei security certificate case, the Federal Court concluded that CSIS had withheld exculpatory evidence from the Court.[14]

- While the security certificate against Mohamed Harkat was ultimately upheld, the Court found that CSIS had withheld information from the Court which showed that key evidence that was presented was unreliable. The Court held that CSIS had undermined the integrity of the court's process and "seriously damaged confidence in the current system."[15]

- The Federal Court found that CSIS was improperly intercepting solicitor-client communications in the Mahjoub case.

All of these issues raise serious questions about whether CSIS can be trusted with greater secret powers when recent history shows there is a pattern of misleading Courts and the Security Intelligence Review Committee.[16]

---

[12] https://www.thestar.com/news/canada/2016/11/03/csis-illegally-kept-sensitive-data-about-people-for-a-decade-federal-court.html

[13] Re X, 2013 FC 1275 at paras. 81, 90-92 and 117-118, 81 and 117 for quotes; and Re X, 2014 FCA 249 at paras. 52-53.

[14] Re Almrei, 2009 FC 1263, paras 502-503

[15] Harkat (Re), [2010] 4 FCR 149, paras 59 and 62

[16] In 2002, former Federal Court Justice James Hugessen presciently expressed reservations about the secrecy of the security certificate regime and the serious risks associated with relying on the candour of CSIS agents: "[P]ersons who swear affidavits for search warrants or for electronic surveillance can be reasonably sure that there is a high probability that those affidavits are going to see the light of day someday. With these national security affidavits, if they are successful in persuading the judge, they never will see the light of day and the fact that something improper has been said to the Court may never be revealed. See James K. Hugessen, "Watching the Watchers: Democratic Oversight" in D. Daubney et al, eds., Terrorism, Law and Democracy: How is Canada Changing Following September 11? (Montreal: Themis, 2002) 381 at 384.

Justification

Finally, there have often been attempts to justify these threat reduction powers by arguing that, at a minimum, agents should have the ability to, during interviews, discourage people from carrying out certain activities, or ask parents to intervene with their children if they believe they are being radicalized. It has been made clear that CSIS has already engaged in these kinds of conversations, before the *ATA* was adopted. If the goal were to simply engage in these kinds of conversations, it would remain debatable about whether an intelligence service is best-suited to carry out these kinds of interventions. In that case, though, we would expect the bill to be drafted to reflect these limited activities. However, both the *ATA* and Bill C-59 grant CSIS powers that go vastly beyond these kinds of interventions. It is imperative that we focus on what this law allows CSIS to do, rather than simply what we are told it will be used for.

Based on the above, as in 2015, we continue to oppose the expansion of CSIS' powers to include threat reduction and disruption activities. We therefore recommend to the committee amend Bill C-59 to repeal CSIS' current threat reduction powers.

2. New powers for CSIS to collect, retain and query datasets

As mentioned in the previous section, in 2016 the Federal Court found that CSIS had been illegally retaining and analyzing data related to non-target individuals. At the time, the ICLMG joined others in denouncing this practice, not just because it breached the law, but because of a fundamental belief that surveillance and data collection, especially when conducted in secret, should be limited to what is strictly necessary for CSIS to carry out its work. At the time, the decision was not challenged, but it was noted that the government left the door open for an eventual legal solution that would allow for CSIS to continue this kind of collection, retention and analysis.[17]

The provisions in Bill C-59 to create new classes of datasets that CSIS can collect, retain and query appear to be such a proposed solution. Bill C-59 creates a wide-ranging system for the authorization of three categories of datasets: data relating to Canadians or people in Canada, data relating to foreign individuals, and publicly available information. Each category has a specific approval process for the collection, retention and querying of the information of each dataset. The most stringent requirements are for information relating to Canadians and people in Canada. This includes seeking out Ministerial authorization to create each class, approval of these authorizations by the Intelligence Commissioner, and, in certain cases, judicial authorization for querying these datasets.

While these safeguards may appear sufficient, we still hold serious reservations about these new powers.

[17] https://www.thestar.com/news/canada/2016/11/03/csis-illegally-kept-sensitive-data-about-people-for-a-decade-federal-court.html

First, we strongly question the government's decision to allow CSIS to broaden the scope of its surveillance activities, from targeting specific people under investigation to targeting entire classes of datasets. This is a clear change in the operations of CSIS to one of potential mass surveillance, collecting vast amounts of information about Canadians and non-Canadians. While there are restrictions placed along the way in terms of what can actually be retained and queried, these do not address the fundamental shift in CSIS' stated operations (although it may reflect what has in fact been occurring with ODAC for the past decade). If CSIS requires such vast powers of data collection, then it is the responsibility of both the Service and the government to make the public case for the necessity of these powers. While we have been active participants throughout the consultation process leading up to the introduction of Bill C-59, we have yet to see such justification. We would therefore suggest to the committee that you seek further clarification before authorizing these new powers.

However, even if the government were to answer these concerns, there are important questions regarding each of the classes of datasets that the Minister will be allowed to authorize CSIS to collect.

Canadians and people in Canada

The restrictions on the retention and querying of these datasets are the strongest of all three categories. However, we do suggest some changes.

First, in section 11.14(2) of the *CSIS Act*, a judge may authorize the retention of a Canadian dataset for up to two years. This appears to be a longer than necessary time period. We would suggest reducing it to one year, with the possibility of requesting an extension, in writing.

It is positive that the Federal Court must authorize retention and set guidelines for querying, etc. However, we would suggest that all Federal Court decisions be sent to the NSIRA for review.

The Act also stipulates in sub section 11.24(3)(d) that the Service shall, for Canadian and foreign datasets:

> (d) verify, periodically and on a random basis, if
> (i) the querying and exploitation of those datasets were carried out in accordance with section 11.2; and
> (ii) the results obtained from the querying and exploitation of those datasets were retained in accordance with section 11.21.

These periodic verifications are what is provided to the NSIRA in order to ensure that querying of datasets is done correctly, and if not the Review Agency must inform the CSIS Director, who must then inform the Federal Court for a decision.

There are two issues with this: one is that "periodic and random" verifications of queries to ensure they are strictly necessary is not stringent enough. Documentation of all queries (including reasons for queries and their results) should be shared with the NSIRA for review, which can flag issues for the Federal Court. Querying is the ultimate use of a dataset and necessitates the strictest level of regulation. Second, ideally this would not be a review, but rather approved beforehand. It is unclear why this is not the case, and we suggest the committee request clarity from the government in order to make proper suggestions. Once a query is completed, and the information used, there is no putting the "genie back in the bottle." If pre-approval is not feasible, then a time period should be placed on NSIRA review of queries at 30 days, to ensure a quick rectification of any issues. Further, the Federal Court should have the power not only to examine the relevance of the query but also any eventual use of that query in order to ensure that ramifications of an illegal query are addressed.

Foreign intelligence

Regarding foreign intelligence datasets, an authorization of five years appears much too long and necessitates further explanation before being enshrined in law. We would recommend that the committee change the authorization limit to one year, with the possibility of extension by the Intelligence Commissioner for another year.

Furthermore, we would suggest stronger thresholds for querying the datasets. Currently, a query would be allowed if it is simply "required" for foreign intelligence purposes. We believe this should also be set to the threshold of "necessary," and that this threshold should also apply when querying Canadian datasets for foreign intelligence purposes. The same issue also applies to the threshold set for the retention of the results of a query: any retention of information should only occur if it is "necessary."

Publicly available information

As detailed in the previous section on the *CSE Act*, we are highly concerned by the ability to authorize the collection of "publicly available information." Bill C-59 places minimal safeguards on the collection, retention, querying or use of "publicly available information." In fact, the proposed amendments to the *CSIS Act* make no attempt to define what "publicly available information" is for the purpose of the dataset. "Relevancy" to CSIS' mandate appears to be the only criteria.

Even with stronger safeguards, concerns about CSIS using "publicly available information" to create vast data banks, without equivalent restrictions on its use, is highly concerning. Similarly to our recommendation regarding the *CSE Act*, we urge the committee to restrict the definition, collection, and use of publicly available information as CSIS datasets. This should include:

- Limiting "publicly available information" to commercially available publications and broadcasts;
- Limiting what can be collected to information that the Intelligence Commissioner

has approved as strictly necessary for CSIS to carry out its mandate.

3. Immunity for acts or omissions that would otherwise constitute an offence

We are also concerned by new powers, to be added as section 20.1 (2) of the *CSIS Act*, granting CSIS agents or individuals at their direction, immunity for "acts or omissions that would otherwise constitute offences." Essentially, this will grant CSIS agents and individuals at their direction the permission to break Canadian law in the pursuit of their activities.

When law enforcement officials were granted these powers in 2001 (in Bill C-24), the proposal was already controversial. At the time, the Canadian Bar Association raised serious concerns, calling it "antithetical to the rule of law."[18] The ICLMG raised similar concerns during the review of Bill C-36, the *Anti-Terrorism Act, 2001*, writing that:

> Even prior to Bill C-36, legislation had been introduced representing an unprecedented expansion of state power under the auspices of fighting organized crime, though never limited in its application only to organized crime. For example, in 2001, Bill C-24, *Criminal Code amendments (Organized Crime)* created an exemption from criminal liability not only for police, but also for agents of the police.[19]

We believe these concerns are even more serious when such powers are given to intelligence agents operating in secret. As with CSIS' threat disruption powers, the issues with granting these powers to CSIS officers are compounded by the fact that, even after the fact, CSIS' actions are unlikely to be revealed or challenged in open court.

Bill C-59 purports to provide oversight to these acts or omissions through the Intelligence Commissioner, but this is applied only to the "classes" of acts or omissions, and on a yearly basis. There is after the fact reporting and review by the NSIRA, and the proposed changes reiterate the need to obtain a warrant in adherence to Section 21 of the *CSIS Act* (which addresses CSIS threat reduction powers).

Despite these attempts at safeguards, they do not off-set the immense danger that granting a spy agency operating largely in secret the power to break the law in the carrying out of their duties.

Moreover, we have seen no public justification from the government about the need for such new powers to be granted. If the government and national security agencies feel that

---

[18] Letter to MP Art Hanger from the CBA, Re: Review of Criminal Code sections 25.1-25.4, June 8, 2006. Online at: https://www.cba.org/CMSPages/GetFile.aspx?guid=fb312e8a-6ec7-4e35-9d66-0261ad57578a

[19] International Civil Liberties Monitoring Group, *In the Shadow of the Law: A Report in response to Justice Canada's 1st annual report on the application of the* Anti-Terrorism Act *(Bill C-36)*, May 13, 2003. Online at: https://interpares.ca/resource/shadow-law

such broad and concerning new powers are necessary, it is incumbent upon them to provide actual evidence of necessity. Barring that, such powers should not be granted.

We therefore urge the committee to remove this section from Bill C-59.

Recommendations

1. That the bill be amended to repeal CSIS' current threat reduction powers.
2. a) That collecting entire datasets be removed from the bill and CSIS' surveillance activities be only targeted to specific people or threats.
   b) If the collection of datasets is kept in the bill, that authorizations for Canadian datasets should be reduced from two to one year, with the possibility of requesting an extension in writing.
   c) That documentation of all queries of Canadian and foreign datasets (including reasons for and results) be shared with the NSIRA for review within 30 days.
   d) That the Federal Court have the power not only to examine the relevance of a query but also any eventual use of that query in order to ensure that ramifications of an illegal query are addressed.
   e) That authorizations for foreign datasets be reduced from five to one year with the possibility of extension for one more year granted only by the Intelligence Commissioner.
   f) That querying datasets for foreign intelligence purposes be only allowed if strictly necessary.
   g) That "publicly available information" be limited to commercially available publications and broadcasts, and its collection only be approved by the Intelligence Commissioner if strictly necessary for CSIS to carry out its mandate.
3. That CSIS agents, and individuals at their direction, not be granted immunity for "acts or omissions that would otherwise constitute offences".

Part 5: The *Security of Canada Information Disclosure Act*

Bill C-51 introduced the *Security of Canada Information Sharing Act* (SCISA). The law legislated the disclosure of Canadians' information between many government departments "if the information is relevant to the recipient institution's jurisdiction or responsibilities […] in respect of activities that undermine the security of Canada".

Bill C-59 renames SCISA to the *Security of Canada Information Disclosure Act* (SCIDA), and brings several changes to the Act. However, these changes do not adequately address the problems with SCISA, in order to protect our privacy, and to prevent its use for undue surveillance and the criminalization of dissent.

First, C-59 modifies the threshold for the disclosure of information to

> "if the disclosing institution is satisfied that (a) the disclosure will contribute to the exercise of the recipient institution's jurisdiction, or the carrying out of its responsibilities […] in respect of activities that undermine the security of Canada; and (b) the disclosure will not affect any person's privacy interest more than is reasonably necessary in the circumstances."

Although a bit of an improvement, "contribute to the exercise of jurisdiction" as well as "reasonably necessary" remain vague and subject to wide interpretation, especially when paired with the overly-broad "in respect to activities that undermine the security of Canada." The result is a clear risk of racial and religious profiling, instead of being limited to the sharing of information on actual threats of violence.

Second, the definition of "activities that undermine the security of Canada" has been somewhat narrowed, but the proposed changes do not go far enough. At first glance, the new definition appears to be an improvement, but in reality it still risks encompassing completely legitimate activities.

Specifically, the bill information sharing powers could still be triggered by activities not posing a real risk to national security, including environmental and Indigenous acts of dissent. For example blocking bridges and roads to protect water and land from dangerous energy projects to which communities have never consented could be seen as being in violation of 3 (f), the "significant or widespread interference with critical infrastructure." It could also potentially encompass activities related to Indigenous sovereignty, land claims and title rights, if they are seen as "undermining the sovereignty and territorial integrity of Canada."

Furthermore, SCIDA would apply to "conduct that takes place in Canada and that undermines the security of another state." This is incredibly vague. We are concerned that this could allow the sharing of information on individuals involved in international solidarity campaigns such as the Boycott, Divestment and Sanction (BDS) movement against products coming from illegal Israeli settlements.

Moreover, the addition of "except if done in conjunction with activity that undermines the security of Canada" to the "exception for art, protest, advocacy or dissent" is a step backward from Bill C-51. As we have shown above, various forms of protest and dissent could be considered as an activity that undermines the security of Canada, therefore triggering SCIDA's powers.

Finally, we are concerned that – even with a stronger exception for dissent and protest – certain Indigenous activities, including actions in support of Indigenous sovereignty, land claims, or title rights, could still be seen as violating the provisions regarding Canadian sovereignty or territorial integrity, and that the committee should consider expanding the exception.

One argument presented in favor of SCIDA is that the sharing of national security related information already occurs between departments, and that this law is an attempt at creating a framework and protecting privacy. In our opinion, the SCIDA reforms do not achieve that goal.

Recommendations

1. SCISA should be rescinded and be replaced by strong privacy protections regulating the sharing of information for national security purposes.
2. Barring this, we recommend that the definition activity that undermines the security of Canada in section 2 be replaced with the following:
   activity that undermines the security of Canada means any activity that threatens the lives or the security of people in Canada or of any individual who has a connection to Canada and who is outside Canada. For greater certainty, it includes
   (a) interference with the capability of the Government of Canada in relation to defense or public safety;
   (b) changing or unduly influencing a government in Canada by force or criminal means;
   (c) espionage, sabotage or covert foreign-influenced activities;
   (d) terrorism;
   (e) proliferation of nuclear, chemical, radiological or biological weapons;
   (f) significant or widespread interference with the global information infrastructure;
   (g) conduct that takes place in Canada and that threatens the lives or security of people in another state.
3. That section 2(1) be replaced with, "For the purposes of this Act, advocacy, protest, dissent or artistic expression is not an activity that undermines the security of Canada unless carried on in conjunction with an activity intended to cause death or bodily harm, endanger life, or cause serious risk to health or public safety."
4. That an exception also be included to cover actions relating to Indigenous sovereignty, land claims, or title rights.

Part 6: Amendments to the *Secure Air Travel Act*

Bill C-59 brings amendments to the *Secure Air Travel Act* in an attempt to address some of its problems. The amendments would:

- Allow parents or guardians be informed if their children are on list
- Allow for a unique identifier that could be used to deal with false-positives
- Allow the government to centralize and manage the list, rather than airlines being responsible for managing and applying the list
- Cause passenger information to be destroyed within 7 days, although with an important exception:

> **Rights preserved**
> 19 For greater certainty, nothing in this Act limits or prohibits the collection, use, disclosure or retention of any information if that collection, use, disclosure or retention is otherwise lawful.

These changes may lead to an eventual improvement in handling false positives and ensuring privacy of travelers' information. However, these amendments do not take the full steps needed to bring about redress for "false positives". Instead, Bill C-59 simply lays the groundwork for possible future regulations. The government should include clear guidelines for the creation of a redress system for false positives. One possibility would be granting the Passenger Protect Inquiries Office (PPIO) the mandate to take immediate steps to establish and manage a redress system. However, as we outline further below, this redress system – already described as complicated and costly – would not be needed if it were not for a flawed and unnecessary no-fly list program.

In our brief on Bill C-51, we outlined the problems with the (then) new SATA legislation. These problems were not rectified at the time. The study of Bill C-59 therefore provides an ideal opportunity to fix these problems:

1. Expanded criteria for listing

In addition to those who pose a threat to transportation security, SATA adds individuals for whom the Minister claims reasonable grounds to suspect that they will travel to commit a terrorist offence abroad. There are other tools that the government may use to prevent those who may be travelling to join foreign conflicts, such as peace bonds or withdrawing one's passport, instead of relying on a regime that has serious due process problems.

2. Listing process

Previously, listing decisions were based on the recommendation of the "Specified Persons List Advisory Group", which included high level officials from the RCMP, CSIS, CBSA, Transport Canada and the Justice Department. Under SATA, the Minister of Public Safety may delegate the listing power to any single official in their department. This removes the extra scrutiny and significance attached to the listing decision that comes with the involvement of several high level officials from different departments and

agencies. The ICLMG submits that listing decisions, if any, should be reviewed and approved by a court of law. Individuals should also be given written notice that they have been added to the no-fly list, and not be left to learn about it from an airline agent when trying to board a plane. No rationale for keeping the listing secret until one attempts to fly has ever been provided and it only serves to maximize the humiliation and harm to dignity, not to mention the cost of losing an airplane ticket.

3. Appeal process

Not only are individuals denied the right to a hearing prior to listing, the appeal process for delisting lacks the procedural due process safeguards that the Constitution demands. Individuals on the list are still denied the right to see the information in their secret file, and are not allowed to cross-examine witnesses who may be sources of information. Notably, Transport Canada's Office of Reconsideration concluded in 2008 that the Passenger Protect Program was plagued with serious problems and contravened section 7 of the *Canadian Charter of Rights and Freedoms* because the people on the list have no right to disclosure, to be heard or to know why they have been targeted.

SATA did not meaningfully address or correct these constitutional shortcomings and we now have an act with provisions that have already been found to violate the *Charter*.[20] It is also important to point out that SATA's appeal process in the Federal Court makes no provision for an independent means to test the Minister's evidence. The Supreme Court of Canada struck down as unconstitutional a similar regime in the security certificate context.

4. Information Sharing

SATA expressly authorizes the Minister to share the list with foreign countries, but does not include any safeguards to ensure the information is relevant, accurate and reliable, or that it won't be shared with a country with a poor human rights record. This provision is particularly troubling because recent history has demonstrated how citizens who Canadian authorities have erroneously labelled as security threats to foreign countries have subsequently been detained and tortured.

5. Unsupported by evidence

There is no evidence that no fly lists improve aviation safety. Travelers on these lists are deemed too dangerous to fly, and yet too harmless to arrest? They are restricted from boarding aircraft, but not trains, ferries, subways, buses, etc.

We have other means of keeping suspected terrorists off airplanes in the Criminal Code:

---

[20] Report for the Office of Reconsideration, October 29, 2008, signed by Allan F. Fenske and Wendy Sutton, Independent Security Advisors, cited in *Report of the Information Clearinghouse on Border Controls and Infringements to Travellers' Rights*, ICLMG, Feb. 2010, p.41. Available at: http://travelwatchlist.ca/updir/travelwatchlist/ICLMG_Watchlists_Report.pdf

- Seeking a peace bond,
- Laying charges (recall, conspiracy to commit, or attempting to commit terrorism offenses are themselves crimes), or
- Seeking a court order for the imposition of a travel ban.

Because our no-fly list regime now closely resembles the US scheme, we have lessons that can be learned from their experience. We know the US list is frequently used to pressure listed individuals to become informants for security agencies. Nothing in the Canadian system, deeply mired in secrecy, protects the public from such abuses.[21]

The amendments in Bill C-59 make an appearance of improving the process. For example, if an individual requests to be removed from the list, the Minister must now respond if the person's request is rejected; no response is deemed to mean that the person is no longer on the list. An individual's right to a response to their request to be removed from a secret list limiting their ability to travel by air is such a basic principle, that it can hardly be seen as an improvement on the system, but rather the granting of a courtesy.

The result is that nothing in Bill C-59 addresses the due process problems at the heart of SATA.

Recommendations

1. That the Safe Air Travel Act be repealed and the Passenger Protect Program be ended.
2. That, barring this:
   a) The government include clear guidelines for the creation of a redress system for false positives.
   b) Decisions to add an individual to the list should be reviewed and approved by a court.
   c) Individuals should be given written notice that they have been listed.
   d) That in defending their listing, an individual and their counsel, have full access to the information and evidence being presented in support of the listing.

[21] https://bccla.org/2016/09/the-new-canadian-no-fly-regime-brought-in-under-the-anti-terrorism-act-2015-aka-bill-c-51/

Part 7: Amendments to the Criminal Code

We are happy to see that the new *National Security Act* would roll back several of the 2015 *Anti-Terrorism Act*'s problematic changes to the Criminal Code. With Bill C-59:

- The provision (brought in by the 2015 ATA) of "promoting terrorism offences in general" would change to "counselling terrorism offenses." This is a much narrower and clearer wording, and won't affect freedom of expression. However, it still seems superfluous because counselling terrorism is already a crime. These provisions should simply be removed.
- Investigative hearings – which were actually introduced with Canada's first *Anti-terrorism Act* in 2001 – would be repealed. Something we wholeheartedly agree with.
- Thresholds for preventative detention (which were lowered with the 2015 ATA) are increased. The change would ensure that an arrest is "necessary" to prevent a crime, rather than simply "likely" to prevent a crime. However, this change should also be applied to peace bonds.

We are, however, concerned that Bill C-59's only change to the "Terrorist Entities Listing" is extending the review period from two years to five years. Any extension of the review period is a regressive change, and placing review at five years is too long a period for review.

We have expressed significant concerns about the entire "Terrorist Entities Listing" program in the past, including its political nature, and its impact on due process and freedom of association. It's very concerning that the only change in Bill C-59 is to weaken rules around the revisions of the list.

Ideally, Bill C-59 would have repealed the "Terrorist Entities Listing" in favour of simply using laws that already prohibit organizations from taking part in criminal activities.

Recommendations

1. That the superfluous and repetitive offence of "counselling terrorism offenses" be removed.
2. That, similar to the changes to preventative detention, the threshold for peace bonds should be increased to "necessary" to prevent a crime.
3. That Bill C-59 should repeal the "Terrorist Entities Listing" in favour of simply using laws that already prohibit organizations from taking part in criminal activities.

Parts 8 & 9: *Youth Criminal Justice Act* & Review of the *National Security Act*

Youth Criminal Justice Act

We are encouraged to see that Part 8 of Bill C-59 offers new protections for the rights of youth involved in terrorism-related offences, by ensuring that any recognizance measures introduced against a youth will go through a youth justice court.

Review

Finally, Part 9 plans a review of Bill C-59 in six years. This is an important safeguard, and we would suggest reducing it to five years for the new oversight and review mechanisms — since it will take time to establish the new offices, etc. — and to three years for the new CSIS and CSE powers. It will be important to ensure that this review happens in an open, public manner, with clear timelines for gathering input from all stakeholders. Recommendations of the review should be binding and fully implemented.

Recommendation:

1. That the review period be reduced to five years for new oversight and review mechanisms and to three years for new CSIS and CSE powers.

What is missing from Bill C-59

1. Review body for the CBSA

NSIRA will cover all national security activities but what of the non-national security related activities of the Canada Border Services Agency (CBSA)? The CBSA is vested with important powers at Canada's border and there have been many complaints formulated against the agency over the years. A strong review mechanism to look at the CBSA and its activities outside of national security has been needed for years and should be created.

2. Security certificates

Security certificates are an immigration proceeding that can be applied to non-citizens who the government decides are a risk to national security and that will lead to the removal of the non-citizen in question.

When challenging a security certificate, neither the named person on the certificate nor their legal counsel has access to the information against them if the government says its disclosure would be "injurious to national security." As a result, neither the individual not their counsel are able to challenge the evidence.

In many cases, non-citizens subject to a security certificate are escaping violence and persecution. Often, if they are returned to their home country, they face detention, torture, disappearance and even death. This is especially true given that they have now been labeled as a suspected terrorist, event though they have never been charged with a crime, let alone convicted of one.

Special advocates – lawyers who have security clearance – have been added in an attempt to make the hearings more fair. They can see the secret evidence, but they do not represent the named person and cannot discuss the evidence with them. Moreover, Bill C-51 limited special advocates' access to information. Bill C-59 does not reverse this damaging change. Although several people have seen the addition of special advocates as an improvement, we argue that overall the security certificates' secret hearings still violate due process and the right to a fair hearing, which can lead to grave consequences.[22]

Bill C-59 should include a provision that puts an end to the security certificate regime.

---

[22] If you haven't done so already, we strongly suggest you watch the documentary *The Secret Trial 5* about the stories of five men who have been subjected to a security certificate and how it gravely impacted their lives. It is available online at: http://secrettrial5.com

3. TUSCAN

Canadian border guards have been screening travellers using a huge, secretive US anti-terrorism database that is almost never referred to publicly. The database, called TUSCAN – which stands for Tipoff US/Canada – is maintained exclusively by the US and is provided to every Canadian border guard and immigration officer, and empowers them to detain, interrogate, arrest and deny entry to anyone found on it.

The TUSCAN list is cloaked in secrecy, and contains the personal information of as many as 680,000 people believed by US authorities to be linked with terrorism. It can be used to prevent individuals from entering Canada and the US by any means – air, water or land. We are aware that the list is used for political reasons, including to bar Canadian activists who are critical of the US administration from entering the United States. Despite Canadian border agents using this list, there is no clear process in Canada to have your name removed from the list. Even if there were a system in Canada, the US would not be required to oblige.[23]

Similar to our position on the Canadian No Fly List, that is should be repealed due to its lack of due process and its violation of mobility rights, we would argue that TUSCAN – a similar but much larger list that has no clear redress process – should not be enforced in Canada. The debate on Bill C-59 provides an opportune moment to address this issue, and we would recommend amending the bill to outlaw the use of TUSCAN by Canadian border agents.

4. The use of the US No Fly List in Canada

We have been privy of numerous cases of Canadian citizens who have recently been prevented from boarding flights to non-US destinations and flights that do not even pass through or near US airspace because of the use of the US No Fly List by air carriers at Canadian airports. Not only would redress be even harder to obtain for Canadians, we argue that it is a violation of Canada's sovereignty for airlines to be using the US No Fly List for flights that are not going to the US and/or are not even passing through its airspace. C-59 should include a provision outlawing the use of the US No Fly List by air carriers for flights leaving Canada that are not going to the US and/or are not passing through its airspace.

Recommendations:

1. That a strong review mechanism to look at CBSA and its activities outside of national security be created.
2. That provisions that put an end to the security certificate regime be included.
3. That a provision outlawing the use of TUSCAN by Canadian border agents be added.

---

[23] https://www.theguardian.com/world/2018/jun/21/canada-us-tuscan-anti-terrorist-database-at-borders

4. That a provision outlawing the use of the US No Fly List by airlines in Canada for flights that are not going to and/or through the US be added.