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

By:
International Civil Liberties Monitoring Group

Presented to:
House of Commons Standing Committee on Public Safety and National Security

January 2018

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. The coalition brings together some 43 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, 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 streets, tens of thousands spoke out, denouncing the process and the content of the bill. The ICLMG and our 45 member organizations were part of the 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 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 relating to Bill C-51 and more broadly.

We were buoyed by the report from the Standing Committee on Public Safety and National Security on its review of Canada's national security landscape. We also welcomed the findings of the third-party analysis of the federal National Security consultation that the vast majority of respondents favoured moves to protect civil liberties and that provisions of Bill C-51 and other powers proposed in the federal Green Paper went a step too far.

While we recognize that Bill C-59 makes efforts in some areas to move in this direction – particularly around new review and oversight bodies, as well as some changes to the criminal code – unfortunately we do not believe it goes far enough. Rather, we see Bill C-59 fitting into the steady progression, since the first 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 when so much is done without public scrutiny or through Canada's transparent and rigorous judicial system.

In the following pages we present what we believe are realistic, necessary recommendations, suggestions and areas of examination that we believe will help to strengthen not just Canadians' rights, but also our security.

List of Recommendations

Part 1: the National Security and Intelligence Review Agency

1. 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).
2. 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.
3. The NSIRA 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.
4. Adding a more specific requirement under "Public Reports" that would mandate a listing of each departmental study requested, and its result.
5. That the NSIRA be granted binding recommendation powers.
6. Mandating an annual follow-up and review on previous recommendations in the NSIRA's annual public reports.
7. That the complaints investigation and reporting mechanisms be amended to ensure greater transparency and accountability; 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

Part 2: The *Intelligence Commissioner Act*

8. The Intelligence Commissioner should be nominated by the Governor in Council, but be approved by a 2/3 vote in the House of Commons.
9. The IC should be appointed on a full-time, rather than part-time, basis.
10. The IC not be restricted to a retired superior court judge, and that the pool should also include active superior court judges.
11. Amend the *Intelligence Commissioner Act* to require the issuance of written reasons when approving any authorization or amendment
12. That the IC be mandated to produce an annual, public report, outlining their activities from the past year, including the number of authorizations reviewed, the number approved and the number rejected, and reasons for those rejections.
13. That the NSIRA be mandated to include a section regarding the work of the Intelligence Commissioner, including an external review of their work.
14. Amending the *Intelligence Commissioner Act* to allow the IC to impose conditions on approved authorizations.
15. Require both approval of the IC and consent of the Minister of Foreign Affairs for all cyber operation authorizations.

Part 3: The *Communications Security Establishment Act*

16. International affairs should be removed from the CSE's cyber operations mandate.
17. That greater restrictions be placed on any CSE activities that are directed at Canadians or people in Canada. In particular, a warrant should be required for any activities related to its technical and operational assistance to other law enforcement and intelligence agencies such as the RCMP and CSIS.
18. Further safeguards should be placed on Active and Defensive cyber operations.
19. Further restrictions be placed on any collection of "publicly available information."
20. Increasing the powers of the Intelligence Commissioner to review all of the CSE's activities.
21. Take steps to further narrow the scope of the CSE's surveillance and cyber activities overall.
22. The *CSE Act* should define metadata; strongly limit its collection, use and retention; and require a warrant to collect it.
23. 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.
24. Any information collected by the CSE should not be retained longer than *necessary* to fulfill the intended objective.
25. Authorizations for foreign intelligence activities should not last for an entire year, and any extension or changes should be examined and approved by the Intelligence Commissioner.
26. To ensure accountability of the CSE, the independence and transparency of the work of the Intelligence Commissioner should be strengthened and, to the greatest amount possible, the CSE's powers and authorizations should narrowly defined.
27. Under no circumstances should the Canadian government – including the CSE – engage in mass surveillance.
28. Any collection of publicly available information should be subject to narrow restrictions, be authorized through Ministerial authorization, and subject to similar safeguards as those for other CSE information collection practices.
29. Impose greater restrictions, including limits on how information is collected, retained, analyzed and disposed of, in the course of the CSE carrying out work in support of the *Investment Canada Act.*
30. Include a limit on how long incidentally acquired information can be retained in the *CSE Act*.
31. The *CSE Act* must enshrine strong privacy protections around CSE's activities into law.
32. Information gathered in order to protect information infrastructure from mischief, unauthorized use or disruption should not be disclosed for any other purpose.
33. Regarding designating persons for the purposes of disclosure of Canadian identifying information, the Minister of Public Safety should report such a

designation and the reasons for it to either the Information Commissioner or Privacy Commissioner, who may then rule on the designation. These reports should also be provided to the NSIRA.

34. Arrangements with foreign countries should be strongly regulated, limited and approved by the Intelligence Commissioner,
35. When sharing information with a foreign country, 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.
36. The Intelligence Commissioner should integrate an analysis of impact on mistreatment or torture into authorization approvals as necessary.
37. Section 56(5) should include an exception preventing a judge from ordering that confidentiality be respected if it hinders due process.
38. Five Eyes spying on each other should be outlawed, and the Canadian government should take actions to that effect.
39. Cyber operation powers are akin to military actions and should be discussed publicly, and further restrictions should be placed on them, including oversight and reporting from the Intelligence Commissioner.
40. The definition of possible cyber operations should be narrowed.
41. Active cyber operations, as well as the creation and use of any cyberweapons, should be strongly limited.

Part 4: Amendments to the *CSIS Act*

42. Amend Bill C-59 to repeal CSIS' current threat reduction powers.
43. Documentation of all queries of Canadian and foreign datasets (including reasons for and results) should be shared with the NSIRA for review within 30 days.
44. The Federal Court should 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.
45. Limit authorizations to one year, with the possibility of extension by the Intelligence Commissioner for another year.
46. Impose stronger thresholds for querying datasets for foreign intelligence purposes.
47. Restrict the definition, collection, and use of publicly available information as CSIS datasets.

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

48. SCISA should be rescinded and be replaced instead by strong privacy protections.

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

49. The government should include clear guidelines for the creation of a redress system for false positives.
50. Listing decisions, if necessary, should be reviewed and approved by a court.
51. Individuals should be given written notice that they have been listed.
52. Ultimately, the Safe Air Travel Act should be repealed.

Part 7: Amendments to the Criminal Code

53. The offence of "counselling terrorism offenses" seems superfluous and should simply be removed.
54. Similar to the changes to preventative detention, the threshold for peace bonds should be increased to "necessary" to prevent a crime.
55. 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.

Part 9: Review

56. Reduce review period to five years for new oversight and review mechanisms and to 3 years for new CSIS and CSE powers.

What's missing from Bill C-59

57. A strong review mechanism to look at the CBSA and its activities outside of national security.
58. Bill C-59 should include a provision that puts an end to the security certificate regime.

Part 1: the National Security and Intelligence Review Agency

The creation of a National Security and Intelligence Review Agency (NSIRA) with an ability to review all government activities related to national security is a very welcome development. We have 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 3 members 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 5 and the maximum number be increased to 8 (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. This would help ensure effective and creative recommendations and reports.

2. Complaint process

The proposal of integrating the complaints process for CSIS, the CSE and 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 considering that the government considers at least 17 government agencies to be involved in national security related operations).

Most glaring 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 review the 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 also plays a key role in national security, particularly regarding Canadians abroad. We believe it should also be included.

We 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. One of these current concerns is the inability of the bodies to make binding recommendations, and the lack of transparency around implementation and follow-up. This has been a particular issue regarding Security and Intelligence Review Committee, where is it unclear from annual reports whether recommendations have been fully implemented, and whether they have been effective in addressing the root of the complaint.

It is understandable that there could be concern around an unelected, appointed body making binding recommendations for a national security agency. However, if we consider that the NSIRA plays a similar role to a Commissioner (and indeed will integrate part of the role of the current CSE Commissioner), it is reasonable for it to have order-making powers. We therefore recommend that the Agency be granted binding powers.

Finally, follow-up and results of the review agency's recommendations could be made more transparent. This could be achieved by mandating an annual follow-up and review on previous recommendations in the NSIRA's annual public reports.

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 Review 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. It is important to note that this restriction is not limited in any way to sensitive or confidential information, but to any "representations made to the Agency by any other person." If it is not sensitive security information, why should they not have access and an opportunity to respond? And we would argue that even with material that is sensitive, the fact that such hearings are held in secret should provide the security necessary to allow the complainant the ability to access and respond to other presentations regarding their complaint.

Second, regarding the reporting of recommendations to the complainant, we would argue that the Agency should be obligated to report all recommendations to the complainant. Again, there is nothing stating that a recommendation can only be withheld because it's sensitive nature; instead, it is simply at the discretion of the Review Agency. This should be revised to mandate that any recommendations made must be reported 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 BCCLA against SIRC regarding a complaint made by environmental organizations regarding CSIS surveillance activities. 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.

This lack of transparency is highly troubling and undermines the review process. This is especially true when coupled with our other concerns outlined above.

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 or recommendations are available to complainants.

Part 2: the *Intelligence Commissioner Act*

Much like the NSIRA, we welcome the proposal of a new Intelligence 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 that this Intelligence Commissioner Act could be improved.

1. Appointment and terms of the Commissioner

It is important that the Commissioner 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, he or she should be appointed on a full-time, rather than a part-time basis.

Finally, we would recommend that the Commissioner 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

The Intelligence Commissioner Act mandates that the Commissioner must report to the NSIRA. However, there is nothing mandating what the NSIRA is to do with these reports. Nor is there a requirement for the Intelligence Commissioner to issue his or her own public reports.

We would make three recommendations:

- Amend the Intelligence Commissioner Act to require the issuance of written reasons when approving any authorization or amendment
- That the Intelligence Commissioner be mandated to produce an annual, public report, outlining their activities from the past year, including the number of authorizations reviewed, the number approved and the number rejected, and reasons for those rejections.
- That the NSIRA be mandated to include a section regarding the work of the Intelligence Commissioner, 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 its ability to effectively oversee the NSA's activities. It is imperative that we learn from this experience and ensure that there is some sunlight in this the Canadian system.

3. Powers

As explained further in the section on the CSE, the Intelligence Commissioner should be required to play a larger role. Therefore we recommend:

- Amending the Intelligence Commissioner Act to allow the Intelligence Commissioner to impose conditions on approved authorizations.
- Require both approval of the Intelligence Commissioner and consent of the Minister of Foreign Affairs for all cyber 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. However, we would like to 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 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. While we are sceptical that "active" cyber operations can be justified for even defensive or security reasons – especially when potential retaliation for such cyber attacks could endanger our security – we definitively do not believe international affairs is a sufficient reason to launch active cyber operations.

Instead, the CSE's mandate should continue to be limited to defence and national security. 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 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, what they believe in, who they talk to, 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 CSE had, in 2013, failed to anonymize Canadians' metadata that it collected while conducting foreign surveillance, and subsequently shared it 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 was 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:

- That greater restrictions be placed on any CSE that are directed at Canadians or people in Canada. In particular, we believe that should a warrant should be required for any activities related to its 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*).
- Further safeguards should be placed on Active and Defensive cyber-operations, which we discuss below.
- That further restrictions be placed on any collection of "publicly available information" – again, discussed further below.

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 pretence 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 legislate 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 a type of 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. 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 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 authorization to allow for the collection of "unselected" information. In essence, unselected information is not tied to any selector (ie, criteria or keyword) – it is what we (along with others) view as

the ultimate form of mass surveillance. 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.

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, that there will be sufficiently strong oversight to either reduce the over-reach we have seen in the past, nor ensure strict controls over the newly expanded CSE powers in 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.[1]

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, be authorized through Ministerial authorization, and subject to similar safeguards as those for other CSE information collection practices.

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 for 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.

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

[1] 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/

are targeted by CSE's activities (again, this would necessitate clarity around what it means for CSE to not "target" Canadians or people in Canada). And more importantly, beyond restrictions on how information is collected, a 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.

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 "back door" 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).[2]

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 needs to enshrine strong privacy protections around CSE's activities into law. The culture of the agency also needs to change, and stronger safeguards than the ones currently proposed by C-59 need to be implemented.

9. Protection of infrastructure

[2] 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.

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 Information 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 the 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 authorization approvals.

12. Confidentiality

Section 56(5) of the CSE Act states that judges must ensure the confidentiality of "(a) 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. This practice is not addressed in the CSE Act.

This practice should be outlawed.

14. New cyber powers

The CSE Act also grants the national security agency new defensive and active cyber operation powers. "Cyber operations" are very concerning, given that they entail activities such as hacking, disrupting of networks, interference with communications, etc.

a. These powers can be triggered solely through a decision by the Minister of National Defense, in consultation with the Minister of Foreign Affairs — it does not require the approval of the Intelligence Commissioner or Parliament. While there are certain restrictions, we believe they are not sufficient. Furthermore, a report on the activities will be shared with the new National Security and Intelligence Review Agency (NSIRA), but with no guarantees that there will be public reporting on these activities. These powers are akin to military actions and should be discussed publicly, and further restrictions should be placed on them, including oversight and reporting from the Intelligence Commissioner.

b. According to the bill, the 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.

c. 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. Offensive hacking can therefore not only make us unsafe because of potential retaliation, these cyberweapons could be leaked, making us the targets of criminals. Active cyber operations, as well as the creation and use of any cyberweapons, should be strongly limited.

Part 4: Amendments to the *CSIS Act*

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

1. Amendments to current threat reduction powers
2. The introduction of a system for CSIS to collect, retain and query specific datasets

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 dome 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 on 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 heightens concerns that these "disruption" powers are unprecedented, dangerous, and have no place in a free and democratic society.

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. At issue is the fact that Bill C-59 does not 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 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:

- Including wording re-iterating the primacy of the Canadian Charter of Rights and Freedoms
- Creating a more clear framework for threat reduction activities by including 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:

<u>Authorization</u>

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 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 over-reach. 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 any kind of 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 issues by creating a set list of actions that limit charter rights and allowing a judge to decide whether a requested 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 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 Agencies. It does mean, however, that the public, civil liberties advocates, and those people targeted by threat reduction activities, 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 with 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 the Service has not yet sought judicial authorization for any threat reduction activity. While on the surface this is positive, the public is still unaware of the nature of the activities, and they will

only become more sensitive as CSIS seeks to carry out activities that require judicial authorization. Given that the powers have only recently been introduced, the time period being examined is also too narrow to give real clarity on how these powers can or will be used. However, if we look to the past, there is a clear list of incidents that raise questions of 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 we have been told SIRC was informed of CSIS' activities, no flags were raised, leading to questions of what information had been shared and when. [3]

- In its 2014-15 annual report, the Security Intelligence Review Committee found that it had been "seriously misled" by CSIS and that CSIS agents had 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 good candour and good faith to the Court had obtained a warrant on the basis of evidence that was deliberately "crafted" to mislead and "keep the Court in the dark".[4]

- In the Almrei security certificate case, the Federal Court concluded that CSIS had withheld exculpatory evidence from the Court.[5]

- While the security certificate against Mohammed Harkat was ultimately upheld, the Court found that CSIS had withheld information from the Court that showed other key evidence that was presented was unreliable. The Court held that CSIS had undermined the integrity in the court's process and "seriously damaged confidence in the current system."[6]

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

---

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

[4] 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.

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

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

All of these questions raise serious questions about whether CSIS can be trusted with greater secret powers when recent history suggests there is a pattern of misleading Courts and the Security Intelligence Review Committee.[7]

Justification

Finally, the need for these threat reduction powers have often been justified 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 been 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 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

[7] 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 that 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 Septemebr 11?(Montreal: Themis, 2002) 381 at 384.

legal solution that would allow for CSIS to continue this kind of collection, retention and analysis.[8]

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 kinds of data sets: data relating to Canadians or people in Canada, relating to foreign individuals, and publicly available information. Each category has a specific approval process for collection, retention and querying of the information the related data sets, the most stringent being 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.

First, we strongly question the government's decision to allow CSIS to broaden the scope of its surveillance activities from those targeting specific investigations, to 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 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.

Even if the government were to satisfy these concerns, we believe that there are important questions regarding each of the classes of datasets that the Minister will be allowed to authorize CSIS to collect.

<u>Canadians and people in Canada</u>

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

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

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 eventual 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 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 and 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 protection. 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.

<u>Foreign intelligence</u>

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 it is placed at simply "required" for foreign intelligence purposes. We believe this should also be set at the threshold of "necessary" (and that this should also apply when querying Canadian datasets for foreign intelligence purposes). The

same also requires to the threshold of "required" being applied to the retention of the information queried; once again, we believe it should be "necessary."

Publicly available datasets

As detailed in the 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," and makes no attempt to define what a publicly available information is for the purpose of the dataset. "Relevancy" to CSIS' mandate appears to be the only criteria (reference to "section 12" of the CSIS Act may invoke strict necessity for querying and use, but unlike other classes of datasets, this is not explicitly stated in Bill C-59, raising questions about whether this is the case).

Even with stronger safeguards, concerns about CSIS using "publicly available information" to create vast databanks, without equivalent restrictions on its use, is highly concerning. We recommend the committee act to restrict the definition, collection, and use of publicly available information as CSIS datasets.

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

Bill C-51 introduced the *Security of Canada Information Sharing Act*. The law legislated the sharing of Canadians' information between many government departments if the information is relevant to an activity that undermines the security of Canada.

The law has been widely denounced. First, "relevant" is a very low threshold, allowing for all kinds of Canadians' private information to be shared without us knowing. Second, SCISA also redefines what is considered an action that "undermines" Canada's national security, broadening it to include interference with "critical infrastructure" and Canada's "economic or financial stability."

Bill C-59 renames the *Security of Canada Information Sharing Act* (SCISA) to the *Security of Canada information Disclosure Act* (SCIDA). Bill C-59 also brings several changes to the Act but these changes are not enough to reverse the problems with SCISA, to protect our privacy, and to prevent its use for surveillance and criminalization of dissent.

Bill C-59 states that "disclosure will not affect any person's privacy interest more than reasonably necessary." This is overly broad and subjective – who will determine what is reasonable? How will that be ensured?

Bill C-59 also clarifies the definition of activities that undermine the security of Canada, which triggers a department being allowed to disclose our private information to another department. It says that to qualify as undermining the

sovereignty, security or territorial integrity of Canada, an activity should constitute "significant and widespread" interference with critical infrastructure. At first glance, this looks like an improvement, but in reality it is still too subjective and vague.

Specifically, the bill could still cover environmental and Indigenous acts of dissent, which often entails blocking bridges and roads to protect water and land from dangerous energy projects that communities have not consented to.

It could also potentially encompass activities related to Indigenous land claims if they are defined 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 or BDS movement against products coming from illegal Israeli settlements.

Furthermore, 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 worse than the previous C-51 exception since we’ve shown above that several manners of protest and dissent can be considered as an activity that undermines the security of Canada.

One argument 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.

SCISA should thus be rescinded and be replaced by strong privacy protections.

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 must 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 this kind of redress. Instead, Bill C-59 simply lays the ground-work 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 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 we not rectified at the time. Review 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, the SATA would add 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 bond conditions or withdrawing one's passport, instead of relying on a regime that has serious due process problems.

2. Process for listing

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 Justice. Under the SATA, the Minister of Public Safety may delegate the listing power to any single official in his or her 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 necessary, should be reviewed and approved by a court. Individuals should also be given written notice the decision has been made, 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 persons on the list have no right to disclosure, to be heard or to know why they have been targeted.

The SATA has not meaningfully addressed or corrected these constitutional shortcomings and we now have an act with provisions that have already been found to violate the Charter. It is also important to point out that SATA's appeal process in the Federal Court makes no provision for a special advocate, or other 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

The 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 labelled as security threats to foreign countries have subsequently been detained and tortured.

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:

- 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.

In our opinion, the *Safe Air Travel Act* should be repealed.

Part 7: Amendments to the Criminal Code

We are happy to see that the new National Security Act would roll back several of Bill C-51's problematic changes to the Criminal Code. With Bill C-59:

- The offence (brought in by C-51) 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 Antiterrorism Act in 2001 – would be repealed. Something we wholeheartedly agree with.
- Thresholds for preventative detention (which were lowered with Bill C-51) 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 2 years to 5 years, which we believe is too long a period and a regressive change.

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.

Part 8: *Youth Criminal Justice Act*

We are encouraged to see that 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.

Part 9: 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 a while to put together the new offices, etc. — and to 3 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 fully implemented.

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 has a lot of powers at our 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". So the counsel cannot challenge the evidence.

Non-citizens subject to a security certificate are often escaping violence and persecution and if they are returned to their home country – with the label of terrorist stuck to them although they have never been charged with a crime, let alone convicted of one – they face detention, torture, disappearance and even death.

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.

On top of all that, Bill C-51 has limited the access to information of special advocates, and Bill C-59 has not reversed 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 and can lead to grave consequences.[9]

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

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